Monad – Leapfrogging Linux With Next Generation Automation

Jeffrey Snover
Architect
Windows Server

FOR MORE INFO...

http://Monad

Context

- System management is a critical problem for MSFT
- Major source of dissatisfaction
- Operational and opportunity costs overwhelm our cost benefit
- Admin/Server ratio stinks
- We consistently misunderstand Admins
  - Allchin's Mom and Dave Cutler
- Linux is kicking our butt

Monad

- Born out of a Convergence of Insights
- UNIX composable management SUCKS
- Economics matter
- .Net Reflection is the next SQL
- We can Leapfrog Linux

UNIX Composable Management

- A | B | C
  - The heart of Unix composable management
- Means that A didn't do what you wanted to do
  - WHY?

UNIX Composable Management

- A | B | C
  - The heart of Unix composable management
- Means that A didn't do what you wanted to do
  - WHY?
- A is a tight coupling of
  - Get Objects => Process Objects => Output as text
  - "| B | C" uses prayer-based parsing to recreate the object so you can do one of the steps differently

UNIX Composable Management

- A | B | C
  - The heart of Unix composable management
- Means that A didn't do what you wanted to do
  - WHY?
- A is a tight coupling of
  - Get Objects => Process Objects => Output as text
  - "| B | C" uses prayer-based parsing to recreate the object so you can do one of the steps differently
- .NET allows us to do better
  - Pipeline structured objects instead of text
  - Pipeline should be between get/process/Output

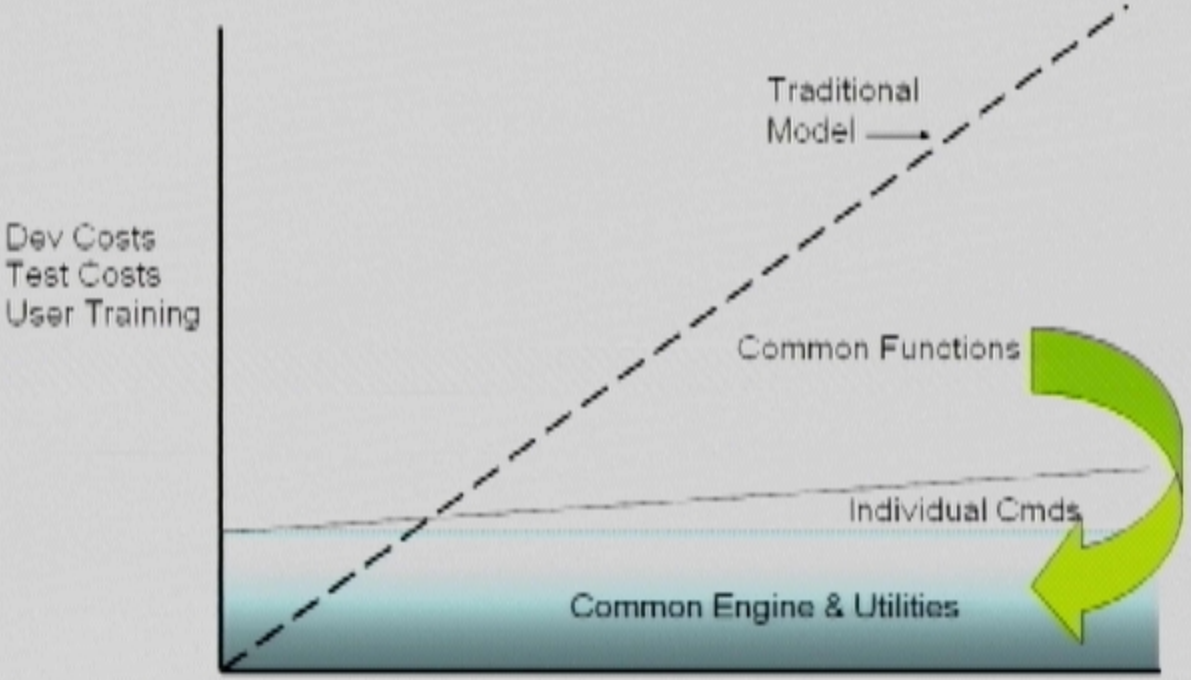
UNIX Composable Management

- A | B | C
  - The heart of Unix composable management
- Means that A didn't do what you wanted to do
  - WHY?
- A is a tight coupling of
  - Get Objects => Process Objects => Output as text
  - "| B | C" uses prayer-based parsing to recreate the object so you can do one of the steps differently
- .NET allows us to do better
  - Pipeline structured objects instead of text
  - Pipeline should be between get/process/Output

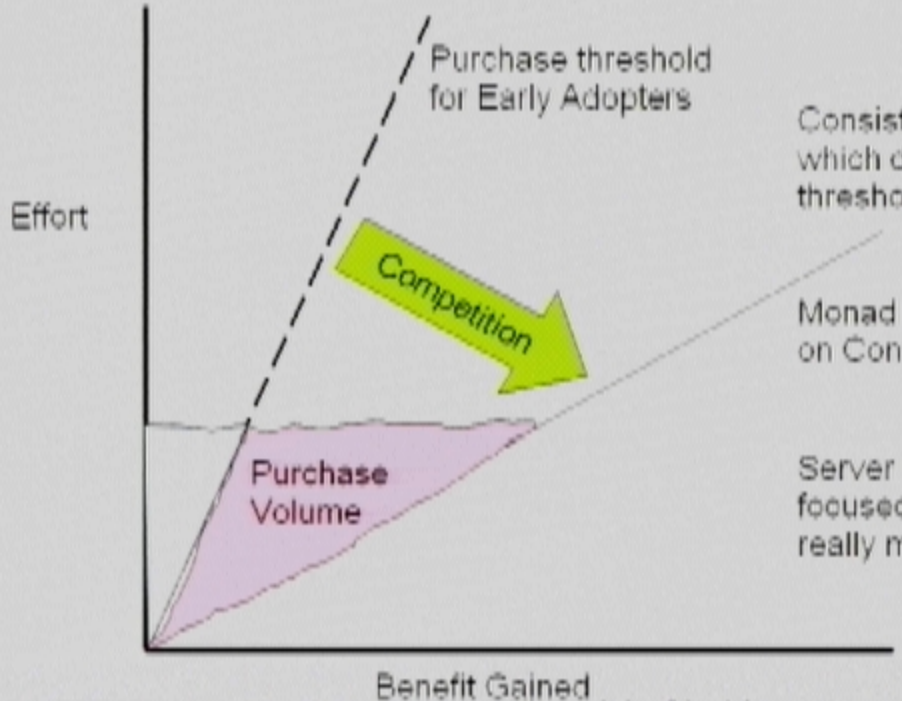
UNIX Composable Management

- A | B | C
  - The heart of Unix composable management
- Means that A didn't do what you wanted to do
  - WHY?
- A is a tight coupling of
  - Get Objects => Process Objects => Output as text
  - "| B | C" uses prayer-based parsing to recreate the object so you can do one of the steps differently
- .NET allows us to do better
  - Pipeline structured objects instead of text
  - Pipeline should be between get/process/Output
- UNIX: Great model – horrible implementation

Economics for Developers



Economics For Customers

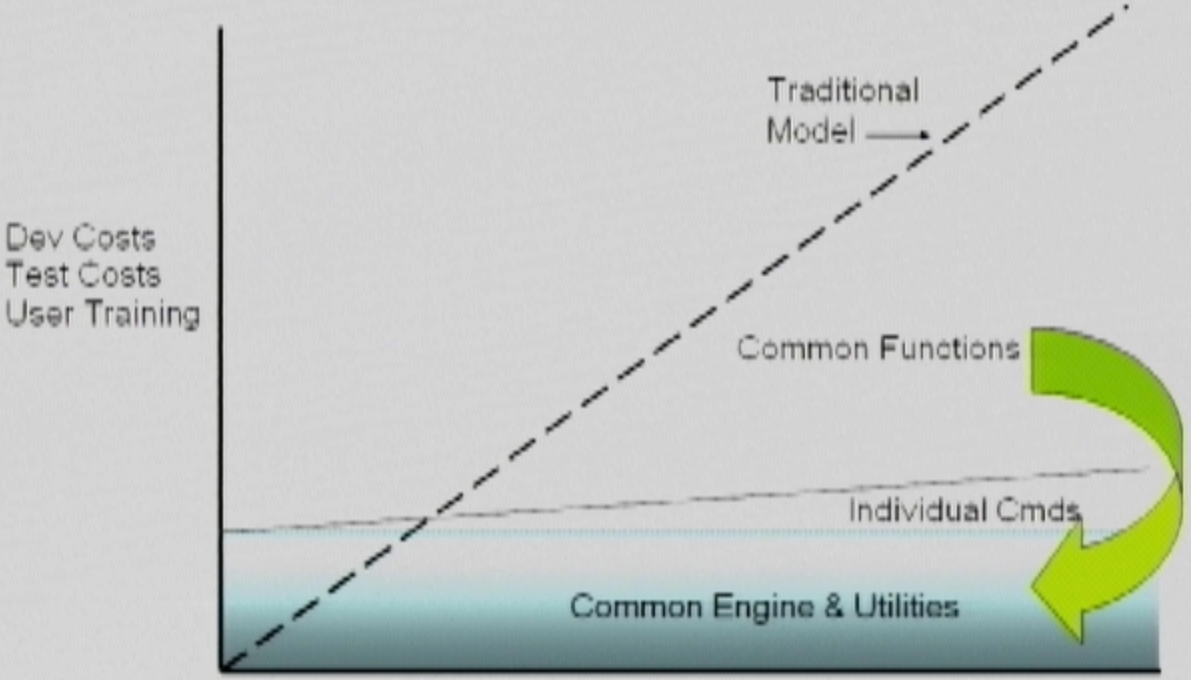


Consistency decreases Effort which decreases purchase threshold

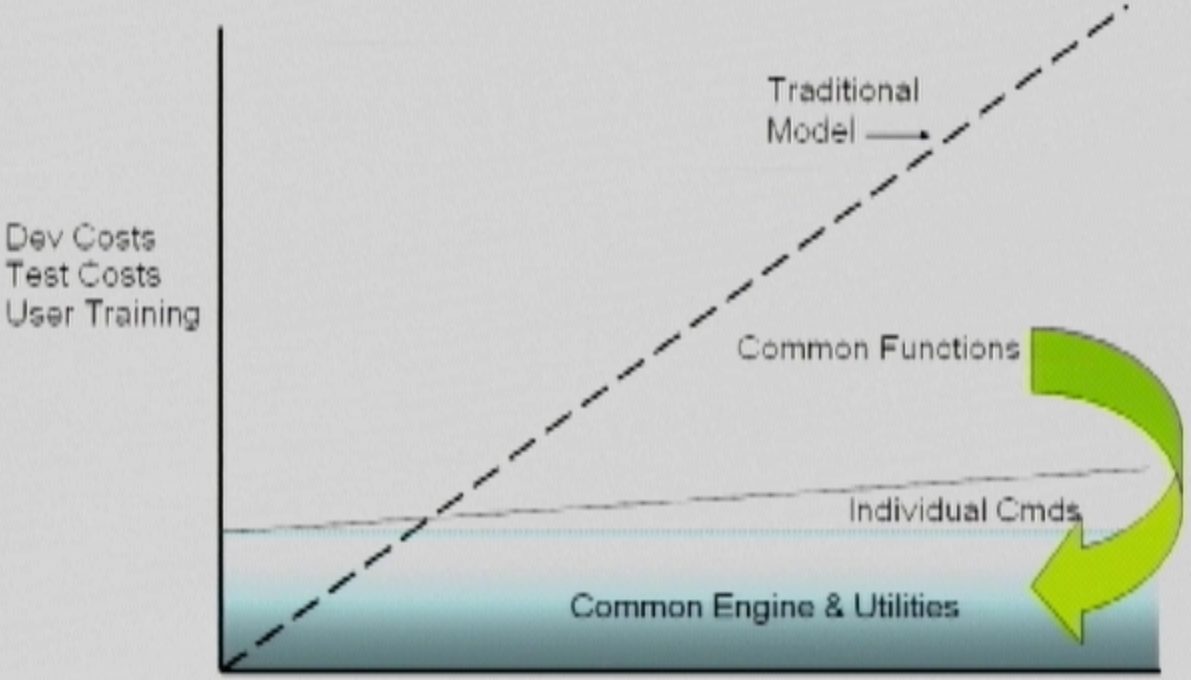
Monad is maniacally focused on Consistency

Server Simplicity efforts on focused on "LESS" which really means Consistency

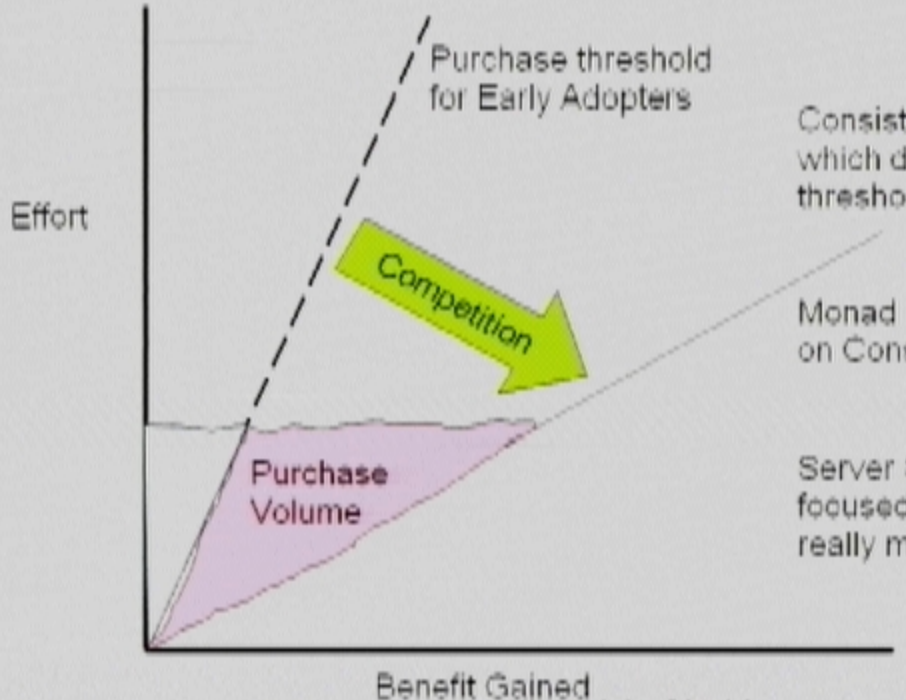
Economics for Developers



Economics for Developers



Economics For Customers



Consistency decreases Effort which decreases purchase threshold

Monad is maniacally focused on Consistency

Server Simplicity efforts on focused on "LESS" which really means Consistency

.Net Reflection is the Next SQL

- UNIX:
  - Standardized data encoding (ASCII files) allows the emergence of a set of domain-neutral utilities for composition and manipulation (e.g. sed, awk, grep)
- SQL:
  - Standardized data forms (Tables) allow the emergence of a set of domain-neutral utilities for composition and manipulation (e.g. join, query, groupby)
- .NET Reflection:
  - Standardized object forms (.net objects) allow the emergence of a set of domain-neutral utitilities for composition and manipulation (MONAD)

Monad Leapfrogs Linux

- As **powerful** and **composable** as UNIX ksh, Perl, and Ruby
- As **consistent** and **production-oriented** as VMS and AS400
- As **embeddable** as TCL

Make Windows admins the most productive in the industry

Big 5 Monad Concepts

1. Commands
   - Classes exposed as CommandLine, API, WS
   - Keep them tiny and leverage MSH to do as much as possible
   - MSH provides parsing, predicate evaluation, data validation, globing, data manipulation
2. Command Family Providers (e.g. navigation)
   - Classes to implement specific sets of functions/Monad provides the Commands
   - Higher levels of semantic/syntactic consistency
3. PropertySets
   - Metadata to give sets of properties standard names
   - Admin friendly abstractions to interact with anything/everything
4. Brokered Methods
   - Methods which provide additional properties or methods to another TYPE
   - Transparent integration of multiple data sources
5. Shared Semantics
   - Set of classes you should use as properties in your classes to facilitate composition and semantic coupling
   - Shifting management from an IS-A to a HAS-A model

Hello World

```
using System.Management.Automation;
namespace MyNamespace
{
    [CommandDeclaration("myhello", "myworld")]
    public class MyCmdlet : Command
    {
        public override void Begin()
        {
            WriteObject( "myhello/myworld: Begin" );
        }
        public override void Execute()
        {
            WriteObject( "myhello/myworld: Execute called: "
            + CurrentObject.ToString());
        }
        public override void Complete()
        {
            WriteObject( "myhello/myworld: Complete" );
        }
    }//Mycmdlet
}//MyNamespace
```

Using Parameters

```
[CommandDeclaration("set", "alias")]
public class SetAliasCommand : AliasCommand
{
    [ParsingMandatoryParameter]
    [ParsingPromptString("Alias Name")]
    [ParsingAllowPipeLineInput]
    [ValidationPattern("[:_a-zA-Z./\\\\][:_a-zA-Z0-9./\\\\]*")]
    [ParsingParameterMapping(0)]
    public string Name;

    [ParsingMandatoryParameter]
    [ParsingPromptString("Substitution string")]
    [ParsingAllowPipeLineInput]
    [ParsingParameterMapping(1)]
    public string Value;
    public override void Execute()
    {
        aliasTable[Name] = Value;
    }
}
```

$ set/alias –name cd –val set/location
$ set/alias cd set/location

$ set/alias
>Alias Name: cd
>Substitution string: set/location

$ ……| set/alias

$ get/alias | set/alias –value XXX

Hello World

```
using System.Management.Automation;
namespace MyNamespace
{
    [CommandDeclaration("myhello", "myworld")]
    public class MyCmdlet : Command
    {
        public override void Begin()
        {
            WriteObject( "myhello/myworld: Begin" );
        }
        public override void Execute()
        {
            WriteObject( "myhello/myworld: Execute called: "
            + CurrentObject.ToString());
        }
        public override void Complete()
        {
            WriteObject( "myhello/myworld: Complete" );
        }
    }//Mycmdlet
}//MyNamespace
```

Using Parameters

```
[CommandDeclaration("set", "alias")]
public class SetAliasCommand : AliasCommand
{
    [ParsingMandatoryParameter]
    [ParsingPromptString("Alias Name")]
    [ParsingAllowPipeLineInput]
    [ValidationPattern("[:_a-zA-Z./\\\\][:_a-zA-Z0-9./\\\\]*")]
    [ParsingParameterMapping(0)]
    public string Name;

    [ParsingMandatoryParameter]
    [ParsingPromptString("Substitution string")]
    [ParsingAllowPipeLineInput]
    [ParsingParameterMapping(1)]
    public string Value;
    public override void Execute()
    {
        aliasTable[Name] = Value;
    }
}
```

$ set/alias –name cd –val set/location
$ set/alias cd set/location

$ set/alias
>Alias Name: cd
>Substitution string: set/location

$ ……| set/alias

$ get/alias | set/alias –value XXX

Parameter Attributes

Predicates
Data Validation

- PrerequisiteMachineRole
- PrerequisiteUserRole
- PredicateScript
- PredicateUIType
- **ParsingMandatoryParameter***
- **ParsingOptionalParameter***
- **ParsingAllowPipelineInput***
- **ParsingParameterMapping***
- **ParsingVariableLengthParameterList***
- ParsingDisallowInteraction
- ParsingRequireInteraction
- ParsingPasswordParameter
- **ParsingPromptString***
- ParsingDefault[Answer,Value]

Parsing
Data Generation

Documentation
Data Presentation

- DocumentName
- DocumentShortDescription
- DocumentLongDescription
- DocumentExample
- DocumentSeeAlso
- DocumentSynopsis
- ValidationRange
- ValidationLength
- ValidationType
- ValidationCount
- ValidationFileAttributes
- ValidationNetworkAttribute
- **ValidationPattern***
- ValidationScript
- **Glob***
- EncodingTypeCoercion

Details available in doc\MetaDataFunctionalSpec.doc or
file://winwebdocs/ntspecs/msh/Monad%20MetaData%20-%20Functional%20Specification.doc

VerbSets

Ubiquitous Verbs	Data Verbs	Lifecycle Verbs	Diagnostics verb
Add	Checkpoint	Disable	Debug
Clear	Compare	Enable	Measure
Copy	Convert	Install	Ping
Get	Export	Restart	Resolve
Lock	Import	Resume	Test
Move	Initialize	Start	Trace
New	Limit	Stop	
Remove	Merge	Suspend	
Rename	Restore	Uninstall	
Set	Update		
Unlock			

Parameter Attributes

Predicates
Data Validation

- PrerequisiteMachineRole
- PrerequisiteUserRole
- PredicateScript
- PredicateUIType
- **ParsingMandatoryParameter***
- **ParsingOptionalParameter***
- **ParsingAllowPipelineInput***
- **ParsingParameterMapping***
- **ParsingVariableLengthParameterList***
- ParsingDisallowInteraction
- ParsingRequireInteraction
- ParsingPasswordParameter
- **ParsingPromptString***
- ParsingDefault[Answer.Value]

Parsing
Data Generation

Documentation
Data Presentation

- DocumentName
- DocumentShortDescription
- DocumentLongDescription
- DocumentExample
- DocumentSeeAlso
- DocumentSynopsis
- ValidationRange
- ValidationLength
- ValidationType
- ValidationCount
- ValidationFileAttributes
- ValidationNetworkAttribute
- **ValidationPattern***
- ValidationScript
- **Glob***
- EncodingTypeCoercion

Details available in doc\MetaDataFunctionalSpec.doc or
file://winwebdocs/ntspecs/msh/Monad%20MetaData%20-%20Functional%20Specification.doc

VerbSets

Ubiquitous Verbs	Data Verbs	Lifecycle Verbs	Diagnostics verb
Add	Checkpoint	Disable	Debug
Clear	Compare	Enable	Measure
Copy	Convert	Install	Ping
Get	Export	Restart	Resolve
Lock	Import	Resume	Test
Move	Initialize	Start	Trace
New	Limit	Stop	
Remove	Merge	Suspend	
Rename	Restore	Uninstall	
Set	Update		
Unlock			

Parameter Sets

Ubiquitous Parameters	Activity Parameters		DateTime Parameters	Format Parameters	Property Parameters	Quantity Parameters	Resource Parameters
Confirm	CaseSensitiv	Force	Accessed	As	Cache	All	Assembly
Culture	Command	Ignore	After	AsScript	Count	Allocation	Application
Description	Compatible	Incremental	Before	AsText	Default	BlockCount	Attribute
Errors	Compress	Insert	Created	Binary	Description	Count	Class
PassThru	Compress	Interactive	Modified	Char	From	Most	Cluster
Scope	Confirm	Interval	Since	Elapsed	Id	Scope	Directory
Verbose	Continuous	Log	TimeStamp	Encoding	Input		Domain
Whatif	Create	Migrate		Exact	LineCount		Drive
	Delete	Notify		Format	Logname		FileName
	Drain	Notify		NewLine	Location		Interface
	Erase	Overwrite		Shortname	Name		IpAddress
	Errors	PassThru		Width	Output		Job
	ErrorLevel	Prompt		Wrap	Owner		Mac
	ErrorLimit	Quiet			Parameter		NodeName
	Exclude	ReadOnly			Password		ParentID
	Exclude	Recurse			Priority		Port
	Fast	Repair			Property		Printer
	Filter	Retry			Reason		Size
	Follow	Select			Regex		TID
	Force	SortBy			Statistic		Type
		Strict			Size		URL
		Temp			Speed		User
		TimeOut			State		
		Trace			Value		
					Version		

Extended Reflection – Drill In

- Enables pipelines of structured data
- Allows access to properties or property paths (e.g. object navigation)
  - E.g. Exename.Version.FileVersion.Major
  - Each section could be:
    - Property/Field
    - Method (with parameters)
    - Xpath specification (for XML docs)
    - Brokered method
- Named sets of properties simplifies the user experience
  - E.g. ConfigurationSet, HealthSet, PerformanceSet, ResourceSet, SecuritySet
  - ConfigurationSet
    - NIC => Name, DeviceID, AutoSense, MACAddress, Speed
    - Service => Name, DesktopInteract, PathName, StartMode, ServiceType, AcceptPause, AcceptStop
- Uniform way to perform formatting Name[:FormatString[:AsName]]
  - E.g. CreationTime:yy-mm-dd:Birthday
- Allows extension of types
  - E.g. Ipaddress.Netview.24HourHealth or Server.Unicenter.ServiceContract.SupportContact
  - Specify a key for a type to enable comparisons

Extended Reflection Drill In

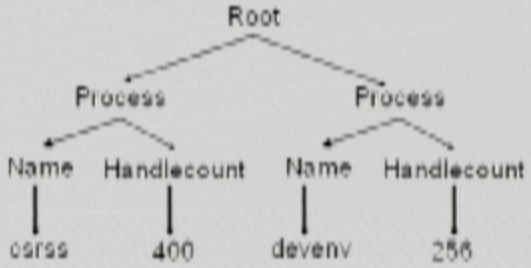
- Normalizes reflection model for .Net, XML, ADO, WMI, ADSI
  - E.g. $ X | total Handlecount

[]Process

Name: csrss Handlecount: 400
Name: devenv Handlecount: 256
Name: svchost Handlecount: 548

DataTable

Name	Handlecount
Csrss	400
Devenv	256
Svchost	548



Extended Reflection does the equivalent of:

```
foreach (process p in ps)
{
 total += p.Handlecount;
}
```

```
foreach (DataRow r in dt.Rows)
{
 total += r["Handlecount"];
}
```

```
foreach (XmlNode n in Root.Children)
{
 total += Int32.Parse(n["Handlecount"]);
}
```

Extended Reflection – Drill In

- Enables pipelines of structured data
- Allows access to properties or property paths (e.g. object navigation)
  - E.g. Exename.Version.FileVersion.Major
  - Each section could be:
    - Property/Field
    - Method (with parameters)
    - Xpath specification (for XML docs)
    - Brokered method
- Named sets of properties simplifies the user experience
  - E.g. ConfigurationSet, HealthSet, PerformanceSet, ResourceSet, SecuritySet
  - ConfigurationSet
    - NIC => Name, DeviceID, AutoSense, MACAddress, Speed
    - Service => Name, DesktopInteract, PathName, StartMode, ServiceType, AcceptPause, AcceptStop
- Uniform way to perform formatting Name[:FormatString[:AsName]]
  - E.g. CreationTime:yy-mm-dd:Birthday
- Allows extension of types
  - E.g. Ipaddress.Netview.24HourHealth or Server.Unicenter.ServiceContract.SupportContact
  - Specify a key for a type to enable comparisons

Extended Reflection Drill In

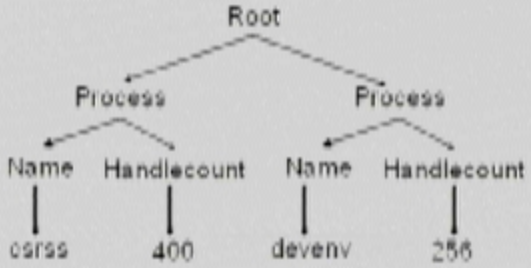
- Normalizes reflection model for .Net, XML, ADO, WMI, ADSI
  - E.g. $ X | total Handlecount

[]Process

Name: csrss Handlecount: 400
Name: devenv Handlecount: 256
Name: svchost Handlecount: 548

DataTable

Name	Handlecount
Csrss	400
Devenv	256
Svchost	548



Extended Reflection does the equivalent of:

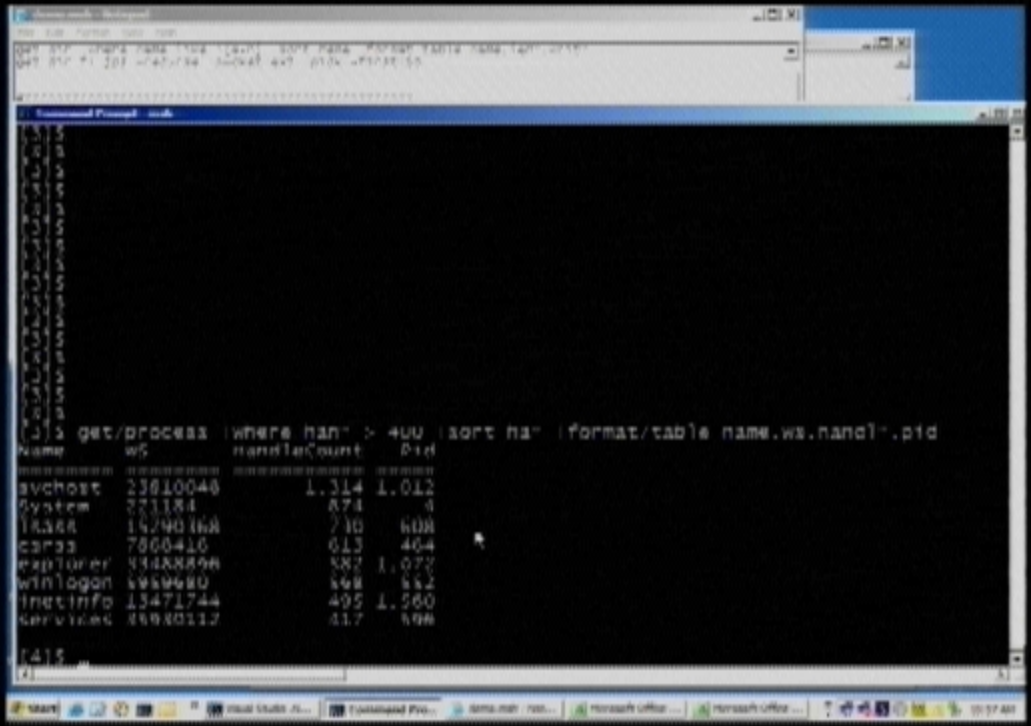
```
foreach (process p in ps)
{
 total += p.Handlecount;
}
```

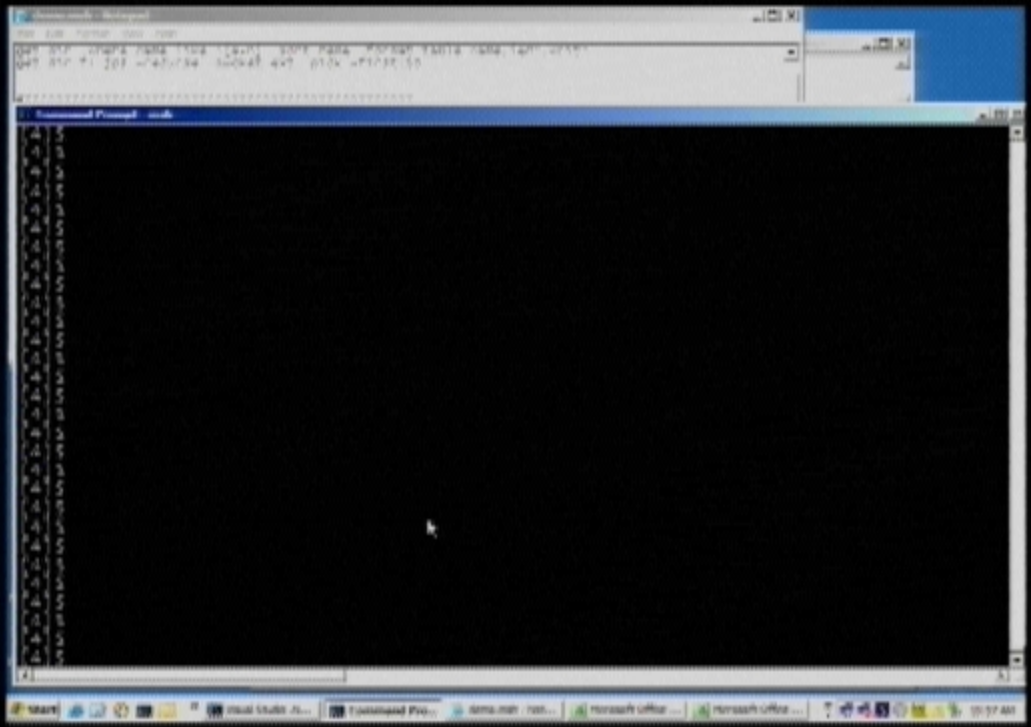
```
foreach (DataRow r in dt.Rows)
{
 total += r["Handlecount"];
}
```

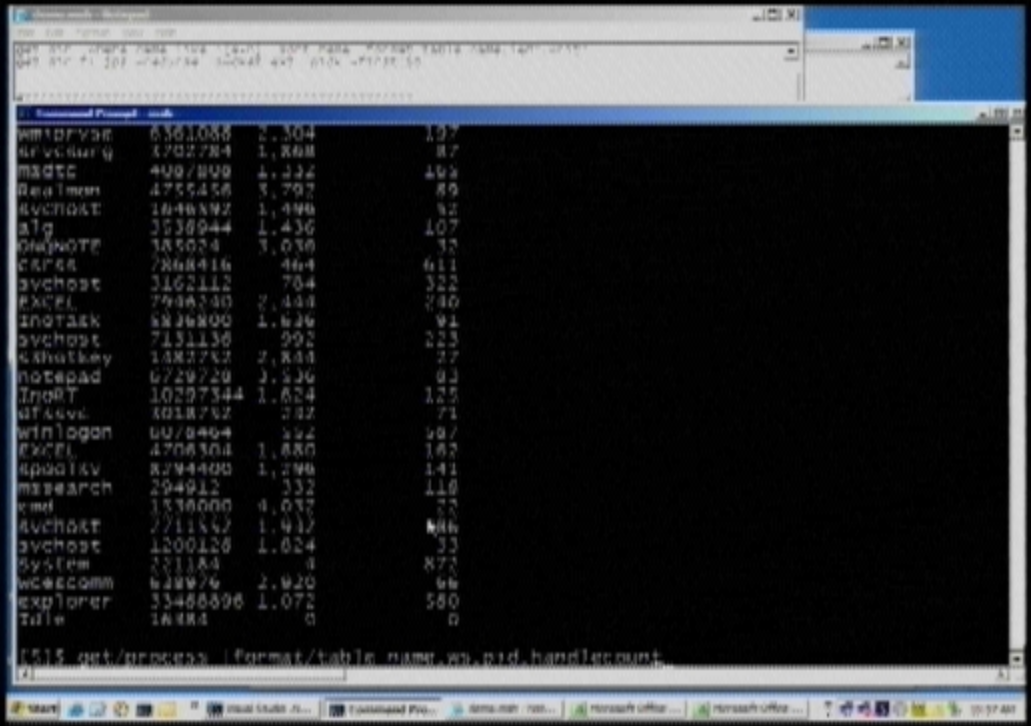
```
foreach (XmlNode n in Root.Children)
{
 total += Int32.Parse(n["Handlecount"]);
}
```

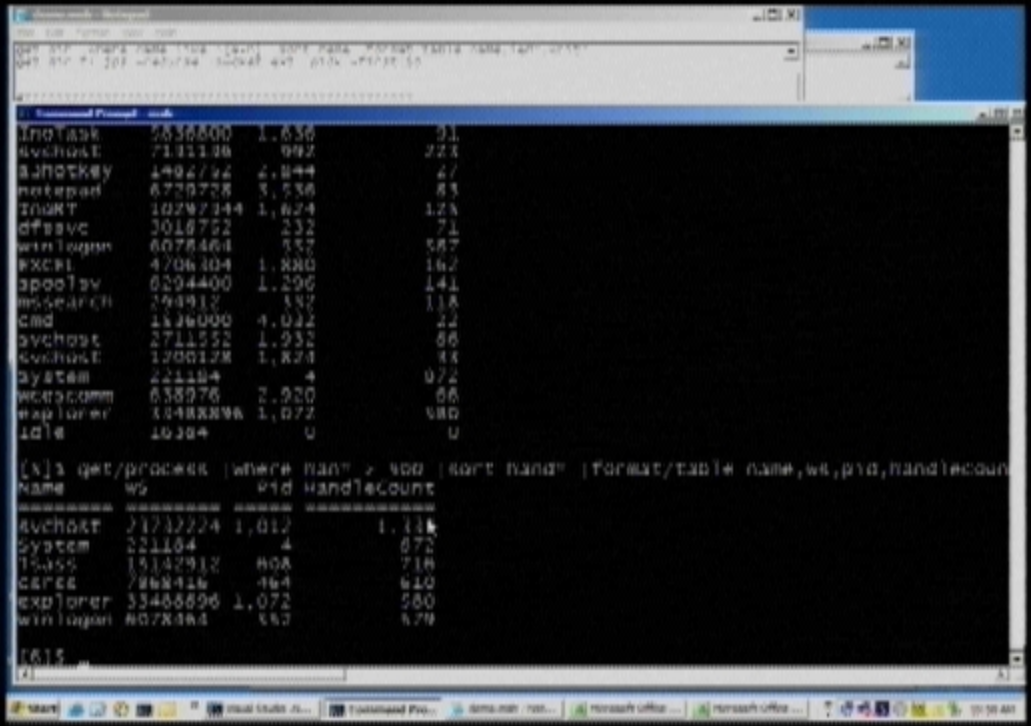
Follow-up

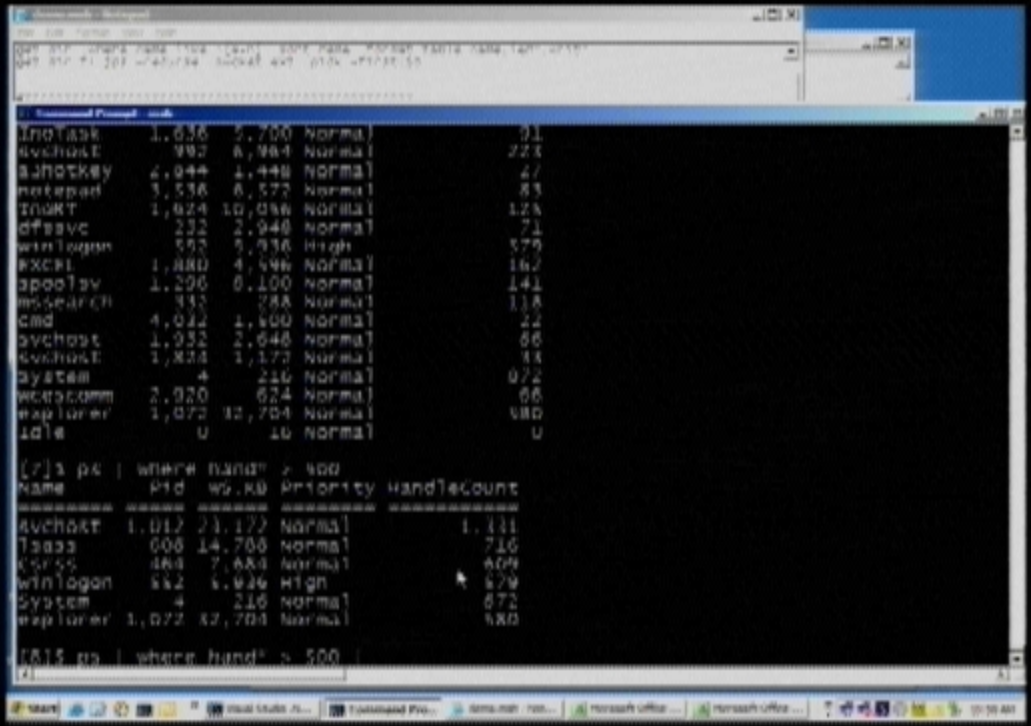
- More Info
  - http://Monad
- Contacts
  - Jeffrey Snover (Architect) jsnover@microsoft.com
  - Daryl Wray (Lead PM) dwray@microsoft.com
- ***Open Positions*** in Redmond
  - Test Manager + 5 SDE/T's
  - 2 PM's (L62+)
  - 2 Dev's (L63+)

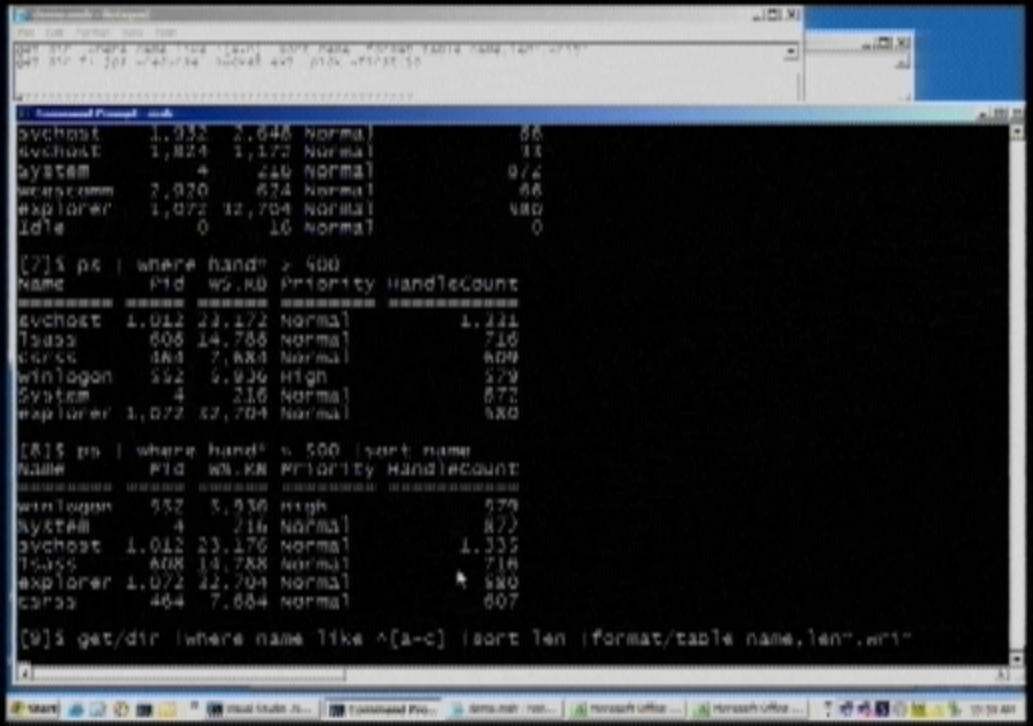

PS C:\> get-process | where hand* > 400 | sort ha* | format-table name,ws,handl*,pid
Name ws handleCount Pid
svchost 23810048 1,314 1,012
System 221184 874 4
lsass 14790868 710 608
csrss 7860416 613 464
explorer 99488896 582 1,072
winlogon 6969680 568 552
taskinfo 15471744 495 1,560
services 8880312 417 596
PS C:\>

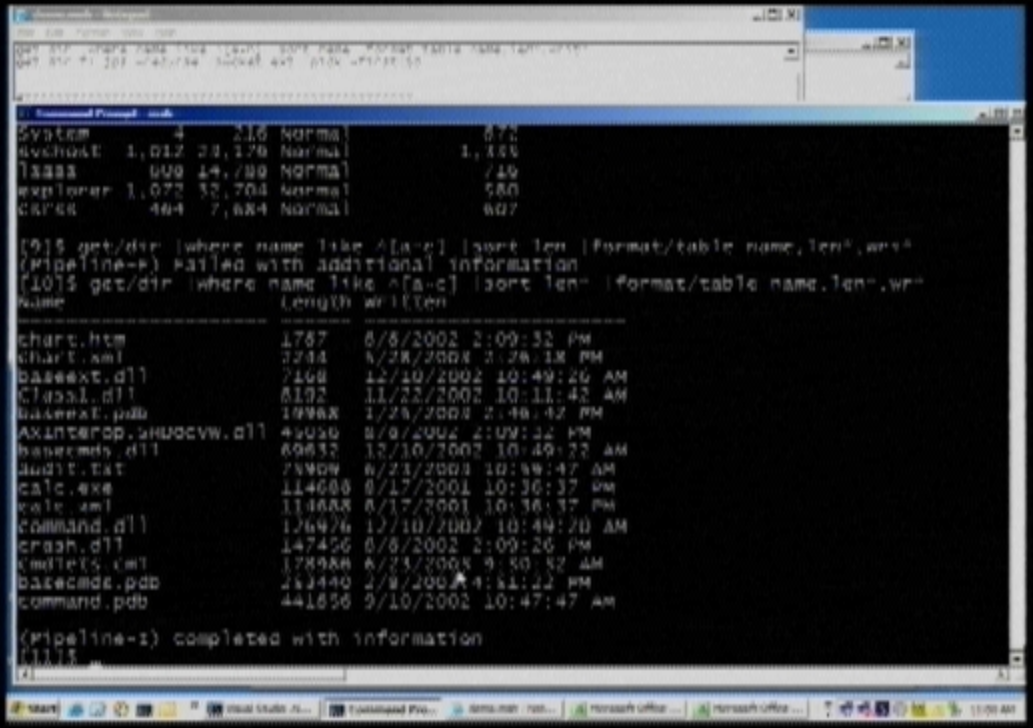


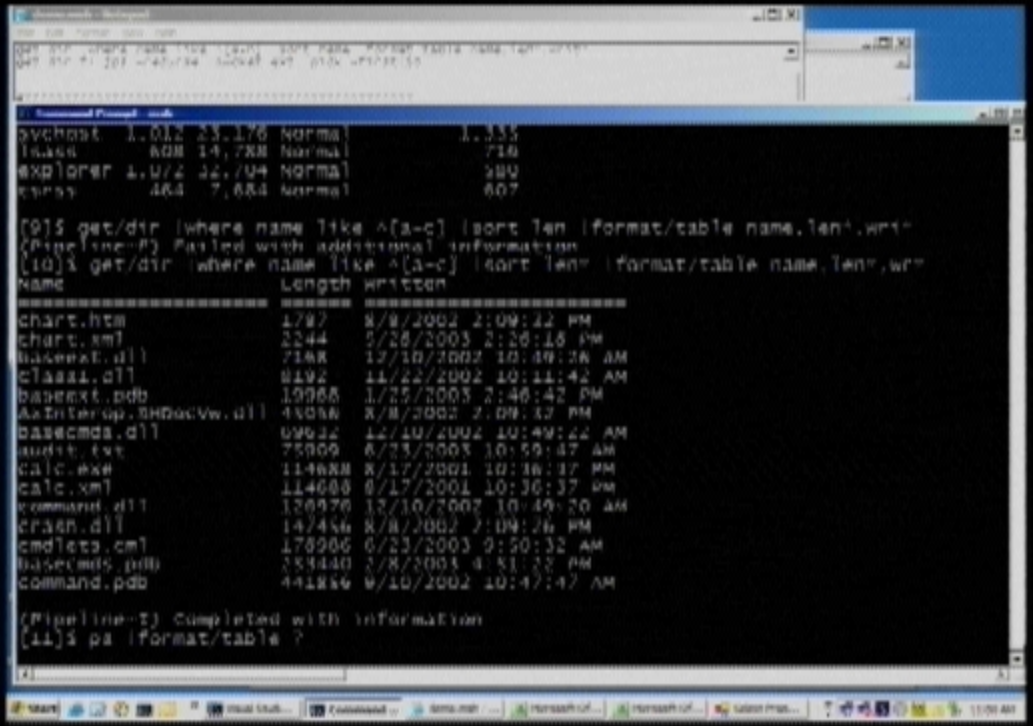

wmiprvse 6361088 2.304 137
srvsvurg 1702784 1.808 87
msdtc 400/808 4.332 403
Realmen 4755456 5.707 89
svchost 1040892 1.400 92
alg 2538944 1.436 107
DWWWOTF 185024 3.030 35
csrss 7868416 464 611
svchost 3162112 704 322
EXCEL 7900240 2.448 780
inotask 6836800 1.620 91
svchost 7131136 992 325
sSHotkey 1382752 2.844 77
notepad 6729720 2.536 83
InoRT 10297344 1.624 125
sftsvc 1018752 392 71
winlogon 6078464 552 287
EXCEL 4706504 1.880 165
spoolsv 8294408 1.700 141
mssearch 294912 332 110
smss 1536000 0.032 22
svchost 7711552 1.912 486
svchost 1200128 1.024 93
System 233184 0 872
wseccomm 6288/6 2.920 66
explorer 33488896 1.072 580
Idle 16384 0 0
C:\> get-process | Format-table name,vm,ws,handlecount

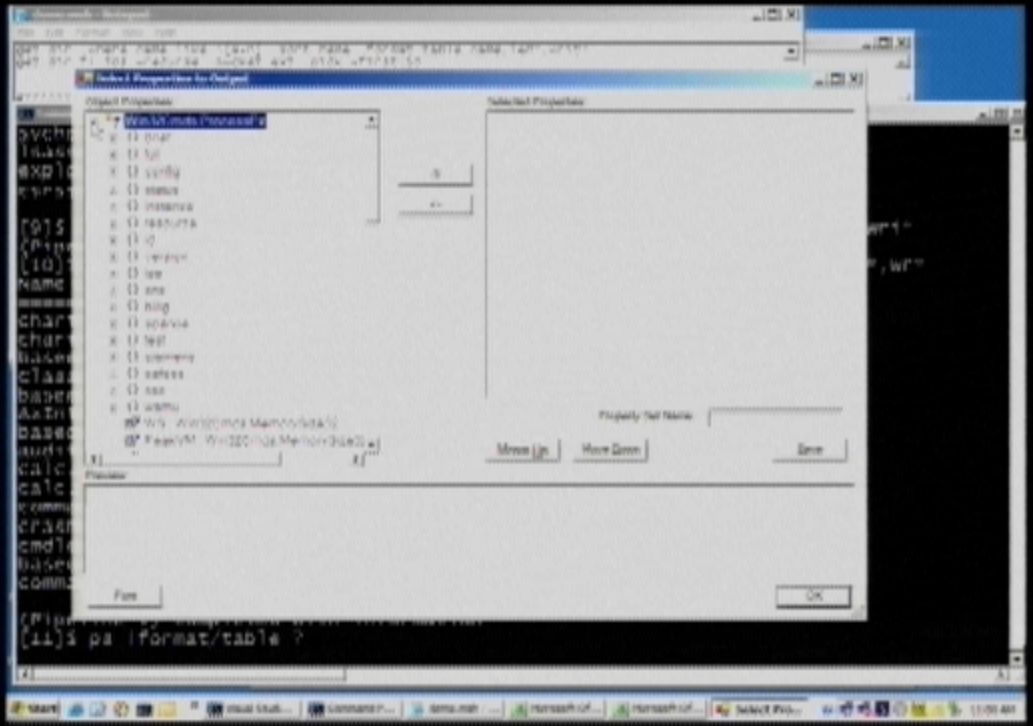

taskmgr 5836800 1,636 31
svchost 71311136 092 224
sidebar 1402732 2,844 27
notepad 6720728 3,536 85
snagit 10297344 1,624 124
dfssvc 3018752 232 71
winlogon 6078464 557 587
excel 4706304 1,880 162
spoolsv 6294400 1,296 141
msseach 290912 592 118
cmd 1536000 4,022 22
svchost 2711552 1,932 86
svchost 1700128 1,824 84
system 221184 4 972
wcescomm 638976 2,920 66
explorer 13488896 1,072 580
idle 16384 0 0
[1]% get/process |where nan" > 400 |sort nand" |format/table name,ws,pid,handlecoun
Name ws pid HandleCount
svchost 21712224 1,012 1,116
System 221184 4 872
lsass 15142912 808 710
csrss 7868416 464 620
explorer 13488896 1,072 580
winlogon 6078464 563 470
[1]%

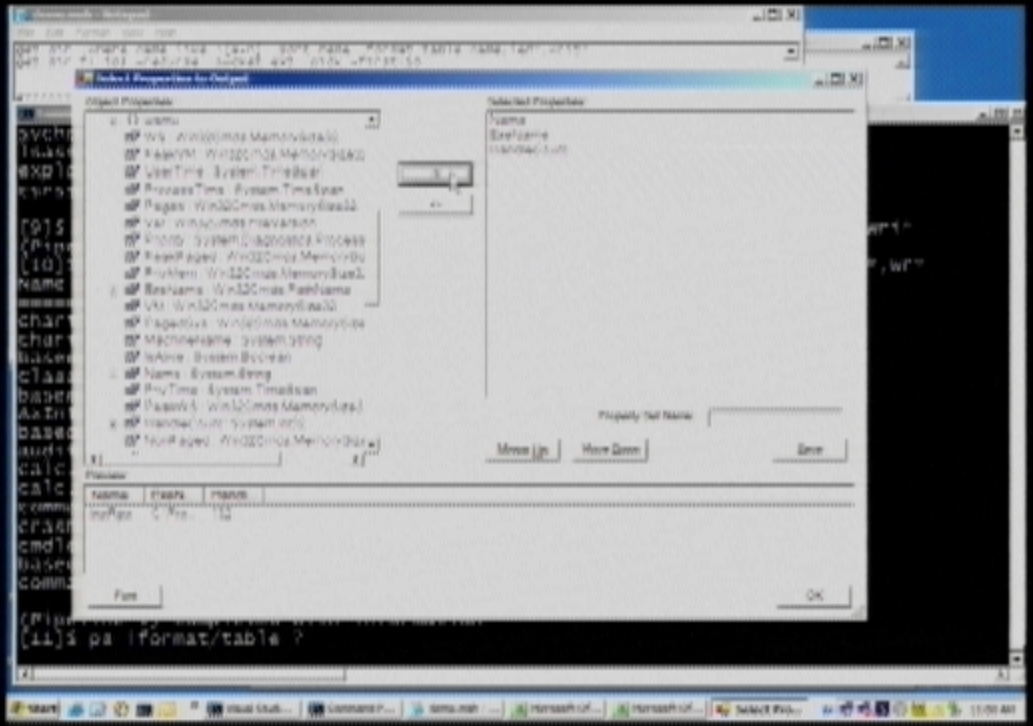

taskmgr.exe 1,636 5,700 Normal 31
svchost.exe 993 8,984 Normal 228
ahotkey.exe 2,044 1,448 Normal 47
notepad.exe 1,536 8,572 Normal 81
tnskt.exe 1,024 10,096 Normal 128
dfssvc.exe 232 2,940 Normal 71
winlogon.exe 592 5,936 High 579
excel.exe 1,880 4,596 Normal 162
spoolsv.exe 1,296 8,100 Normal 141
msearch.exe 992 788 Normal 118
cmd.exe 4,012 1,600 Normal 22
svchost.exe 1,932 2,648 Normal 86
svchost.exe 1,836 1,172 Normal 84
system 4 216 Normal 872
wscntfy.exe 2,020 624 Normal 66
explorer.exe 1,072 12,704 Normal 480
idle 0 16 Normal 0
[7]% ps | where handlecount > 500
Name Pid WS.KB Priority HandleCount
svchost.exe 1,012 21,172 Normal 1,111
lsass.exe 608 14,708 Normal 716
csrss.exe 464 7,684 Normal 609
winlogon.exe 592 5,936 High 579
System 4 216 Normal 872
explorer.exe 1,072 12,704 Normal 480
[8]% ps | where handlecount > 500

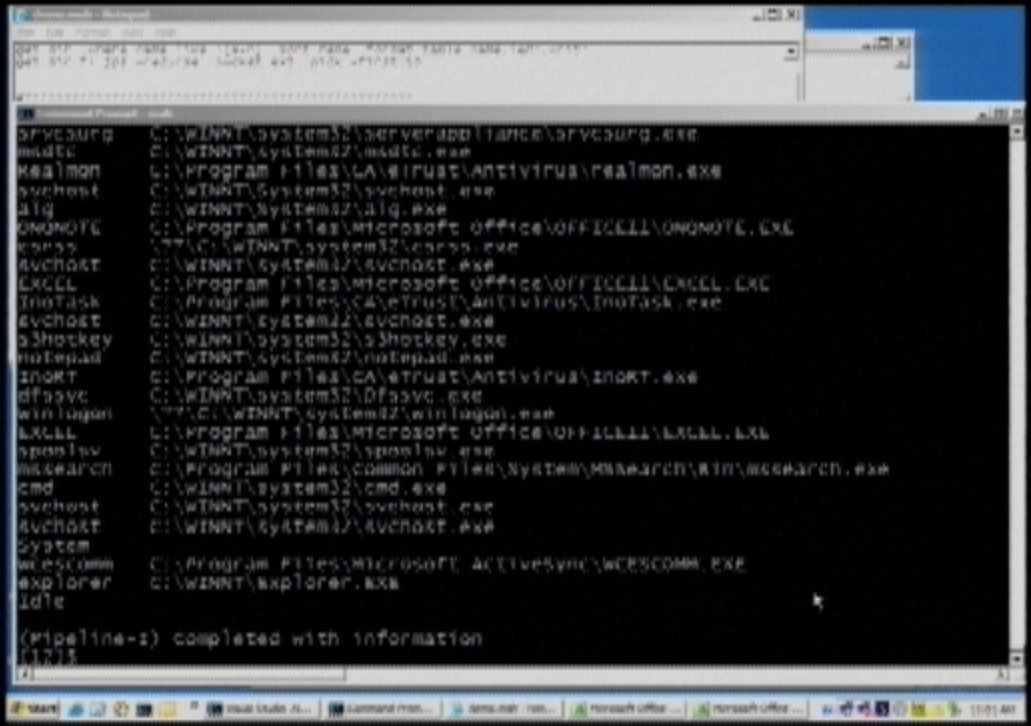

svchost 1,852 2,648 Normal 66
svchost 1,824 1,172 Normal 11
System 4 216 Normal 972
wmiprvse 2,070 674 Normal 66
explorer 1,072 12,704 Normal 980
Idle 0 16 Normal 0
[7]$ ps | where hand* > 600
Name Pid WS.KB Priority HandleCount
svchost 1,012 23,172 Normal 1,111
Tsass 608 14,788 Normal 716
csrss 464 7,684 Normal 609
winlogon 552 5,936 High 579
System 4 216 Normal 872
explorer 1,072 12,704 Normal 980
[8]$ ps | where hand* > 500 |sort name
Name Pid WS.KB Priority HandleCount
winlogon 552 5,936 High 579
System 4 216 Normal 872
svchost 1,012 23,176 Normal 1,333
Tsass 608 14,788 Normal 716
explorer 1,072 12,704 Normal 980
csrss 464 7,684 Normal 607
[9]$ get/dir |where name like ^[a-c] |sort len |format/table name,len".wri"

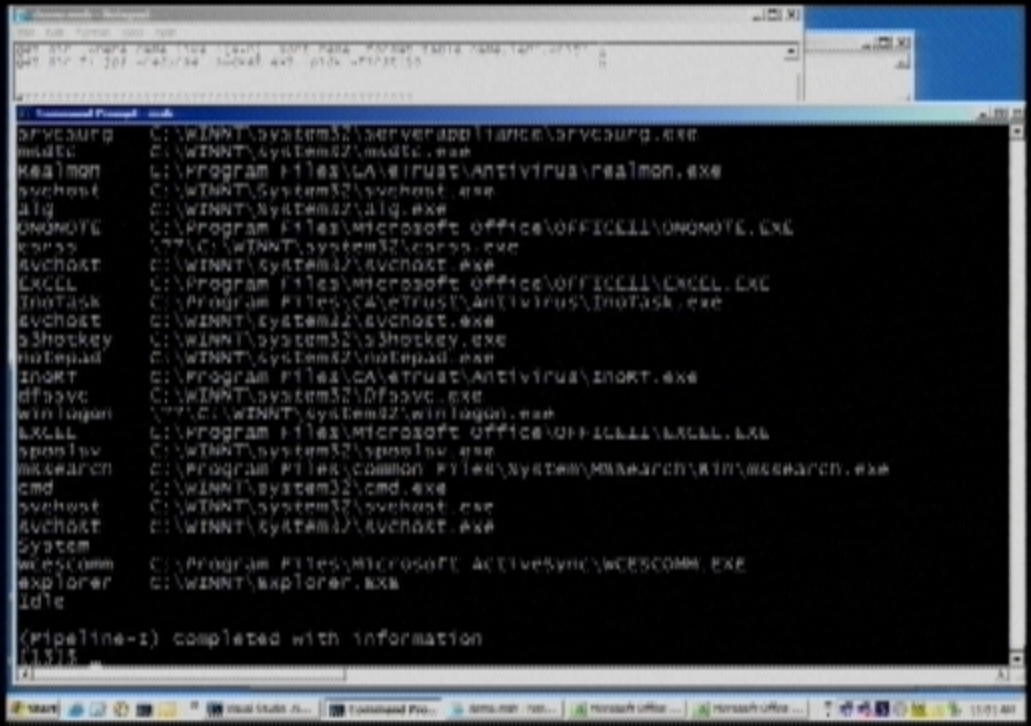

System 4 216 Normal 0%
svchost 1,012 38,176 Normal 1,16%
Idle 0 24,00 Normal 0%
explorer 1,072 52,704 Normal 0%
csrss 404 7,884 Normal 0%
[9]$ get/dir |where name like ^[a-c] |sort len |format/table name,len*,wri*
(Pipeline-5) failed with additional information
[10]$ get/dir |where name like ^[a-c] |sort len* |format/table name,len*,wr*
Name Length Written
chart.htm 1787 8/8/2002 2:09:32 PM
chart.xml 3244 8/28/2002 3:26:18 PM
baseext.dll 7168 12/10/2002 10:49:26 AM
CTapal.dll 8192 11/22/2002 10:11:42 AM
BaseExt.pdb 19968 1/25/2004 2:40:42 PM
AxInterop.SHDocVw.dll 46080 8/8/2002 2:09:32 PM
basecmds.dll 69632 12/10/2002 10:49:22 AM
audit.txt 79909 8/23/2003 10:59:47 AM
calc.exe 114688 8/17/2001 10:36:37 PM
calc.xml 114688 8/17/2001 10:36:37 PM
command.dll 126976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.xml 178986 8/23/2003 9:50:52 AM
basecmds.pdb 253440 2/8/2004 4:51:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(Pipeline-1) completed with information
[11]$

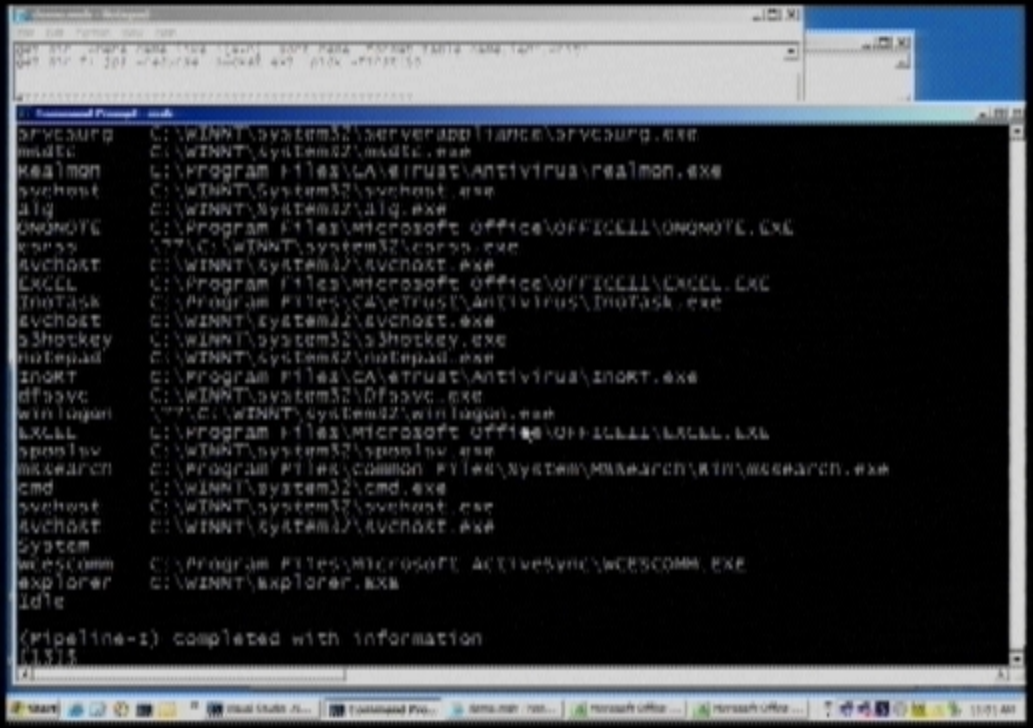

[9]$ get/dir |where name like ^[a-c] |sort len |format/table name,len".wr"
(Pipeline-8) Failed with additional information
[10]$ get/dir |where name like ^[a-c] |sort len" |format/table name,len",wr"
Name Length Written
chart.htm 1797 8/8/2002 2:09:22 PM
chart.xml 2244 5/28/2003 2:36:16 PM
basecmds.dll 77824 12/10/2002 10:49:20 AM
classa.dll 8192 11/22/2002 10:11:42 AM
basecmds.pdb 139968 1/23/2003 2:46:42 PM
calc.exe 114688 8/17/2001 10:36:37 PM
calc.xml 114688 8/17/2001 10:36:37 PM
command.dll 126976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.cml 178906 6/23/2003 9:50:32 AM
basecmds.pdb 253440 2/8/2003 4:51:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(Pipeline-11) Completed with information
[11]$ ps |format/table ?

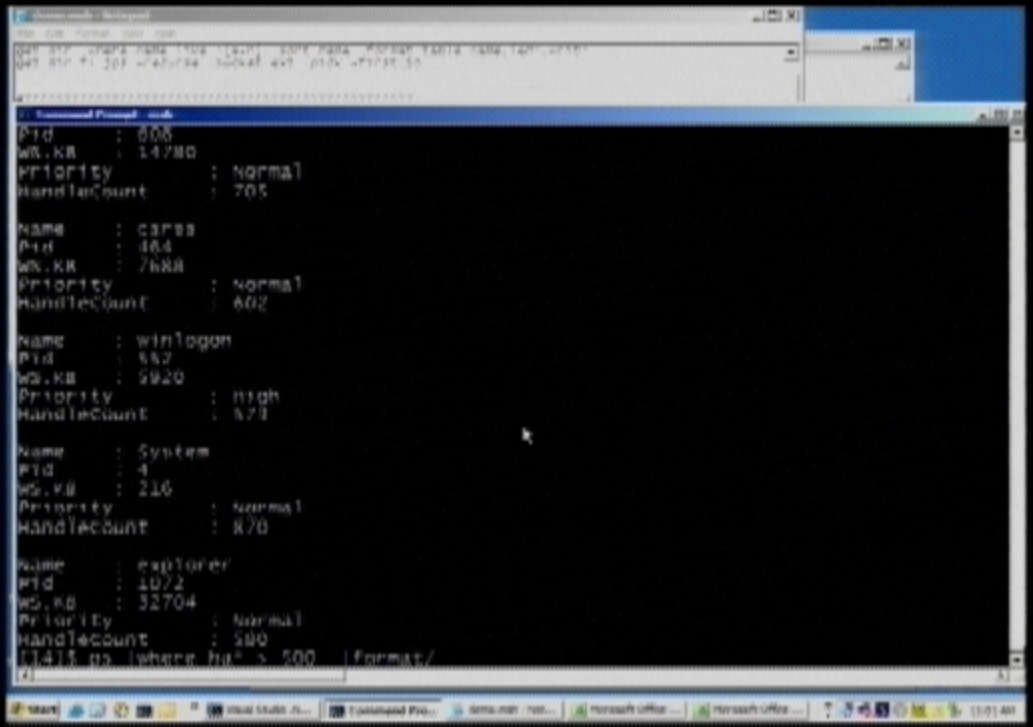

Object Properties
Selected Properties
Property Set Name:
Move Up
Move Down
Save
Preview
Print
OK
[ii]$ ps |format/table ?

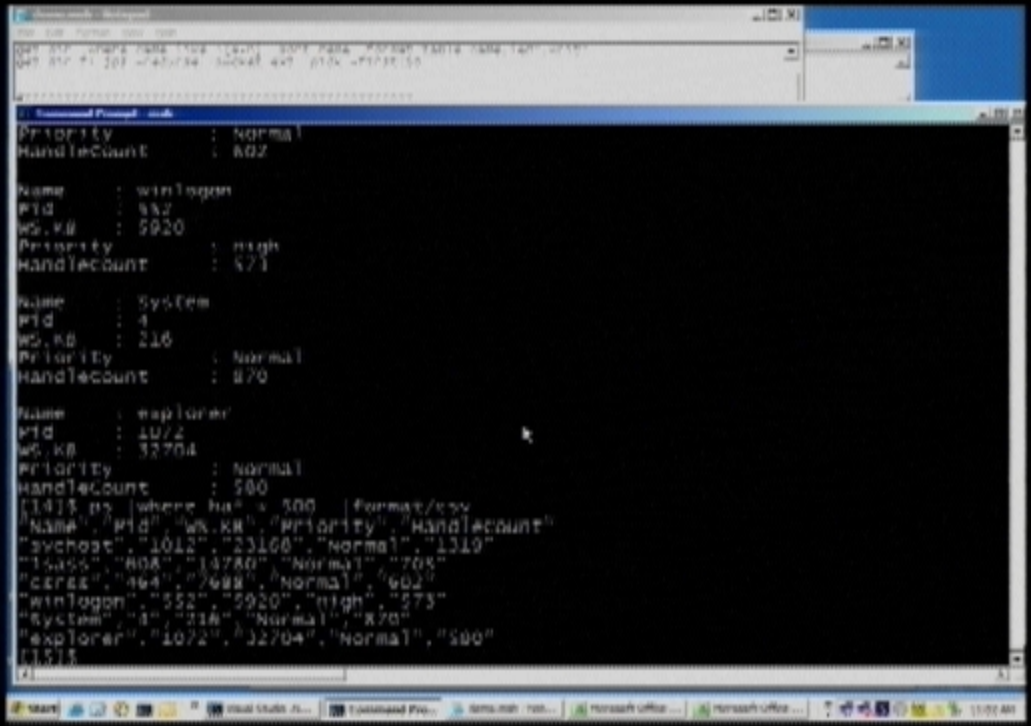

Object Properties
Selected Properties
Name
Forename
Move Up
Move Down
Save
Preview
Form
OK
[ii]$ ps |format/table ?

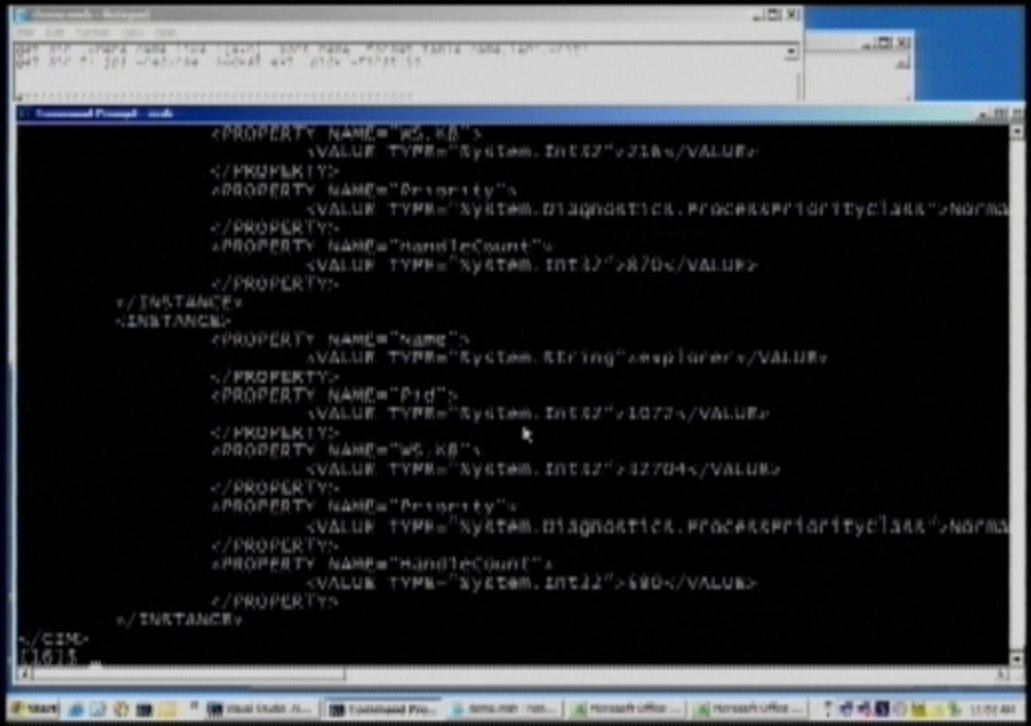

srvcsurg C:\WINNT\system32\serverappliance\srvcsurg.exe
msdtc C:\WINNT\System32\msdtc.exe
realmon C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost C:\WINNT\System32\svchost.exe
alg C:\WINNT\System32\alg.exe
ONENOTE C:\Program Files\Microsoft Office\OFFICE11\ONENOTE.EXE
csrss \??\C:\WINNT\system32\csrss.exe
svchost C:\WINNT\system32\svchost.exe
EXCEL C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost C:\WINNT\System32\svchost.exe
s3Hotkey C:\WINNT\system32\s3Hotkey.exe
notepad C:\WINNT\System32\notepad.exe
InoRT C:\Program Files\CA\eTrust\Antivirus\InoRT.exe
dfssvc C:\WINNT\system32\Dfssvc.exe
winlogon \??\C:\WINNT\System32\winlogon.exe
EXCEL C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv C:\WINNT\system32\spoolsv.exe
msdearch C:\Program Files\Common Files\System\MSSearch\Bin\msdearch.exe
cmd C:\WINNT\system32\cmd.exe
svchost C:\WINNT\system32\svchost.exe
svchost C:\WINNT\System32\svchost.exe
System
wcescomm C:\Program Files\Microsoft ActiveSync\wCESCOMM.exe
explorer C:\WINNT\explorer.exe
Idle
(Pipeline-1) completed with information

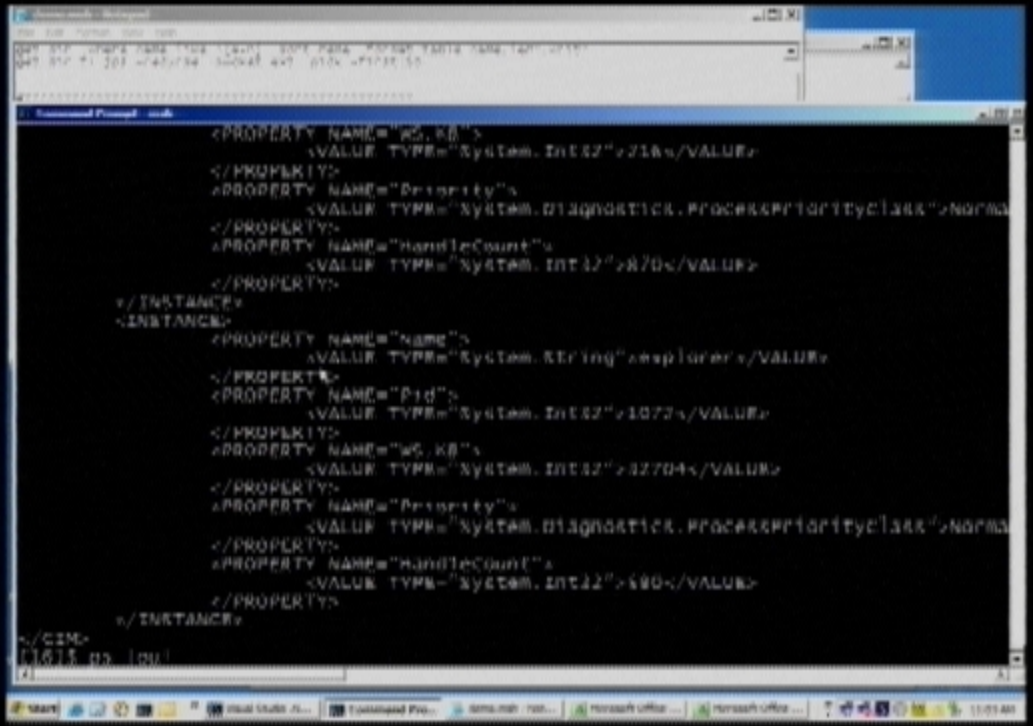

srvcsurg C:\WINNT\system32\serveradplance\srvcsurg.exe
msdtc C:\WINNT\System32\msdtc.exe
realmon C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost C:\WINNT\System32\svchost.exe
alg C:\WINNT\System32\alg.exe
ONENOTE C:\Program Files\Microsoft Office\OFFICE11\ONENOTE.EXE
csrss \??\C:\WINNT\system32\csrss.exe
svchost C:\WINNT\system32\svchost.exe
EXCEL C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost C:\WINNT\System32\svchost.exe
s3Hotkey C:\WINNT\system32\s3Hotkey.exe
notepad C:\WINNT\System32\notepad.exe
InoRT C:\Program Files\CA\eTrust\Antivirus\InoRT.exe
dfssvc C:\WINNT\system32\Dfssvc.exe
winlogon \??\C:\WINNT\System32\winlogon.exe
EXCEL L:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv C:\WINNT\system32\spoolsv.exe
MSSearch C:\Program Files\Common Files\System\MSSearch\BIN\MSSearch.exe
cmd C:\WINNT\system32\cmd.exe
svchost C:\WINNT\system32\svchost.exe
svchost C:\WINNT\System32\svchost.exe
System
wcescomm C:\Program Files\Microsoft ActiveSync\WCESCOMM.EXE
explorer C:\WINNT\explorer.exe
Idle
(Pipeline-1) completed with information

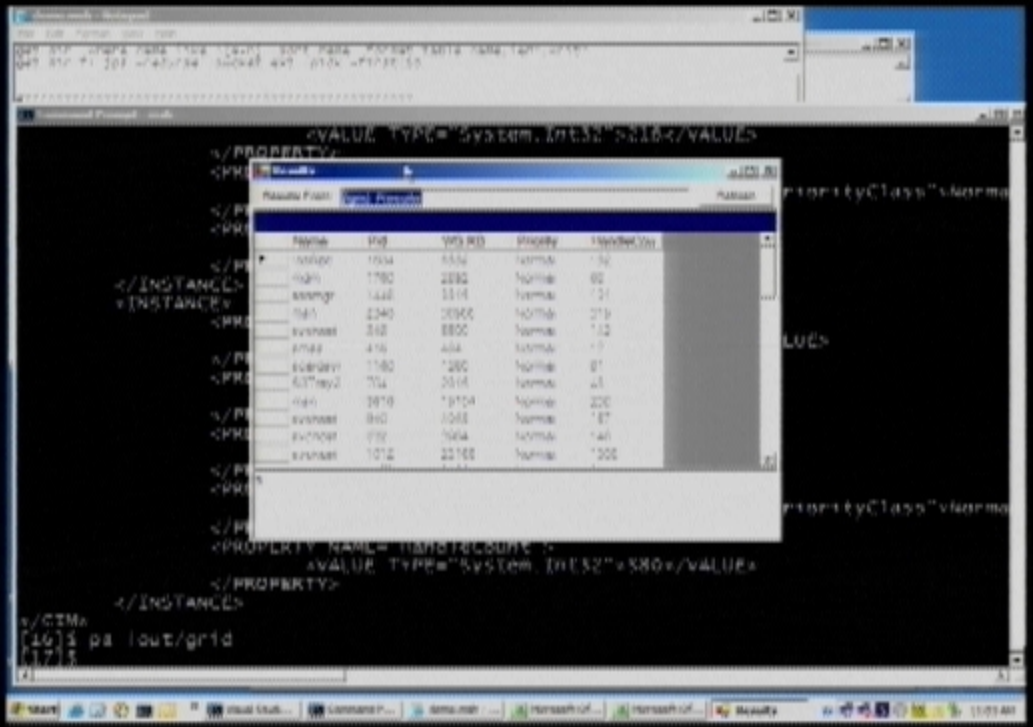

C:\Command Prompt - cmdc
srvcsurg C:\WINNT\system32\serveradministance\srvcsurg.exe
msdtc C:\WINNT\System32\msdtc.exe
realmon C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost C:\WINNT\System32\svchost.exe
alg C:\WINNT\System32\alg.exe
ONENOTE C:\Program Files\Microsoft Office\OFFICE11\ONENOTE.EXE
csrss \??\C:\WINNT\system32\csrss.exe
svchost C:\WINNT\system32\svchost.exe
EXCEL C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost C:\WINNT\System32\svchost.exe
s3Hotkey C:\WINNT\system32\s3Hotkey.exe
notepad C:\WINNT\System32\notepad.exe
InoRT C:\Program Files\CA\eTrust\Antivirus\InoRT.exe
dfpsvc C:\WINNT\system32\Dfpsvc.exe
winlogon \??\C:\WINNT\System32\winlogon.exe
EXCEL C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv C:\WINNT\system32\spoolsv.exe
MSSearch C:\Program Files\Common Files\System\MSSearch\BIN\MSSearch.exe
cmd C:\WINNT\system32\cmd.exe
svchost C:\WINNT\system32\svchost.exe
svchost C:\WINNT\System32\svchost.exe
System
wcescomm C:\Program Files\Microsoft ActiveSync\wCESCOMM.EXE
explorer C:\WINNT\explorer.exe
Idle
(Pipeline-1) completed with information

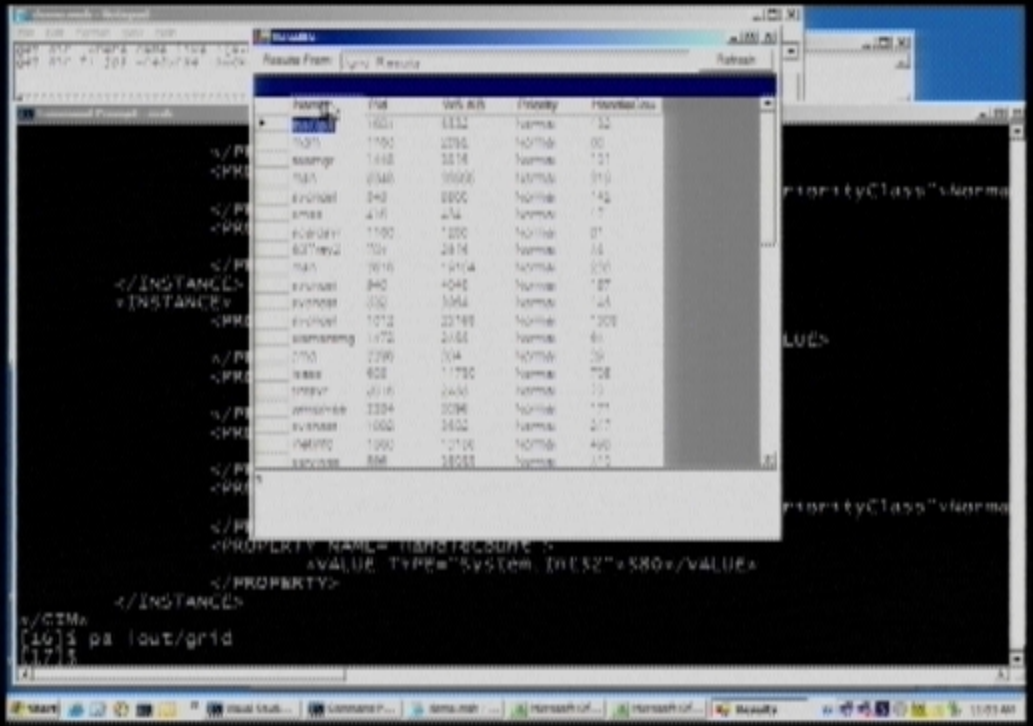

Pid : 608
WN.KB : 14780
Priority : Normal
HandleCount : 705
Name : csrss
Pid : 464
WN.KB : 7688
Priority : Normal
HandleCount : 602
Name : winlogon
Pid : 552
WS.KB : 5920
Priority : High
HandleCount : 570
Name : System
Pid : 4
WS.KB : 216
Priority : Normal
HandleCount : 870
Name : explorer
Pid : 1072
WS.KB : 32704
Priority : Normal
HandleCount : 590
[1413 gs |where hu* -s 700 |format/

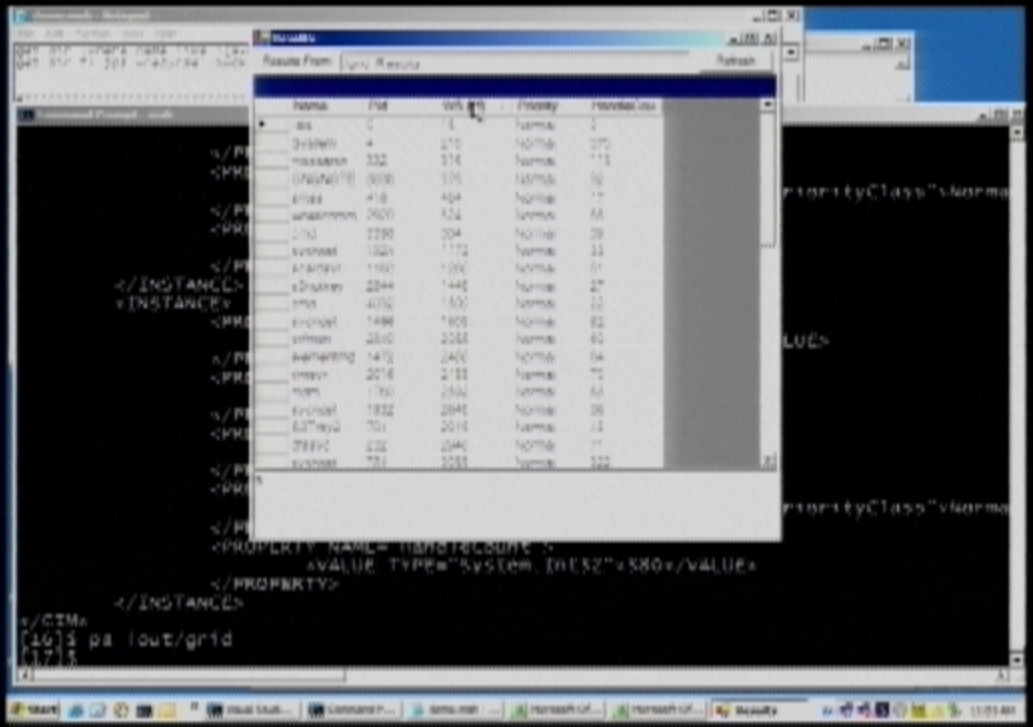

Priority : Normal
HandleCount : 602
Name : winlogon
Pid : 552
WS.KB : 5920
Priority : High
HandleCount : 573
Name : System
Pid : 4
WS.KB : 216
Priority : Normal
HandleCount : 870
Name : explorer
Pid : 1072
WS.KB : 32704
Priority : Normal
HandleCount : 500
"Name","Pid","WS.KB","Priority","HandleCount"
"svchost","1012","23160","Normal","1319"
"lsass","808","14780","Normal","705"
"csrss","464","7688","Normal","602"
"winlogon","552","5920","High","573"
"System","4","216","Normal","870"
"explorer","1072","32704","Normal","500"

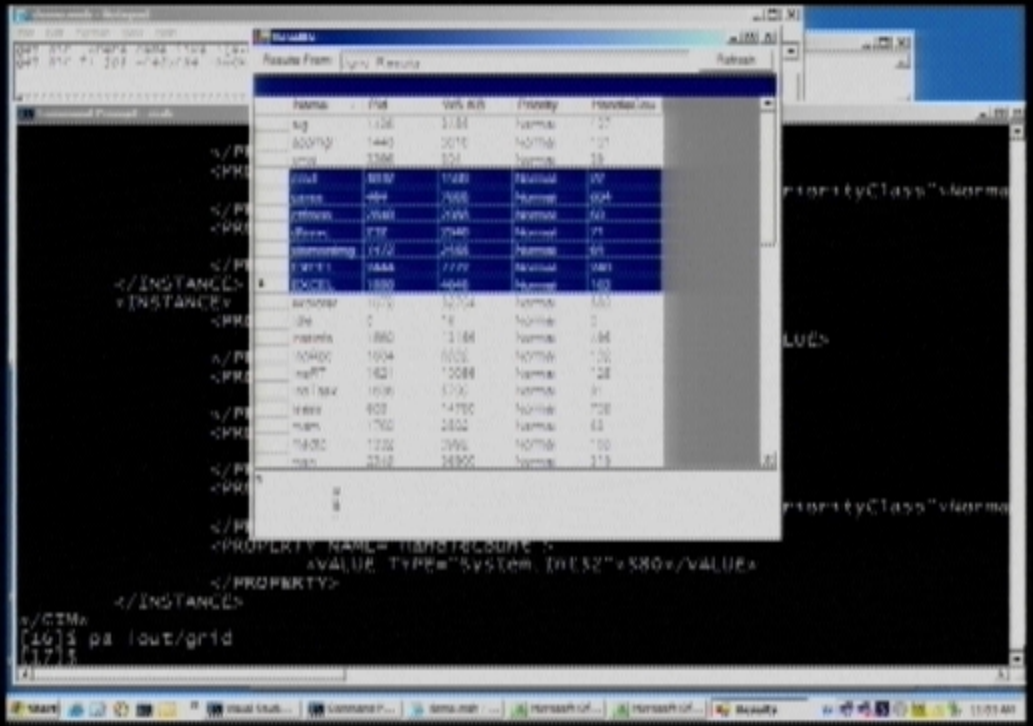

<PROPERTY NAME="WS,KB">
<VALUE TYPE="System.Int32">716</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Norma
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">870</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">explorer</VALUE>
</PROPERTY>
<PROPERTY NAME="Pid">
<VALUE TYPE="System.Int32">1077</VALUE>
</PROPERTY>
<PROPERTY NAME="WS,KB">
<VALUE TYPE="System.Int32">42704</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Norma
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">680</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>

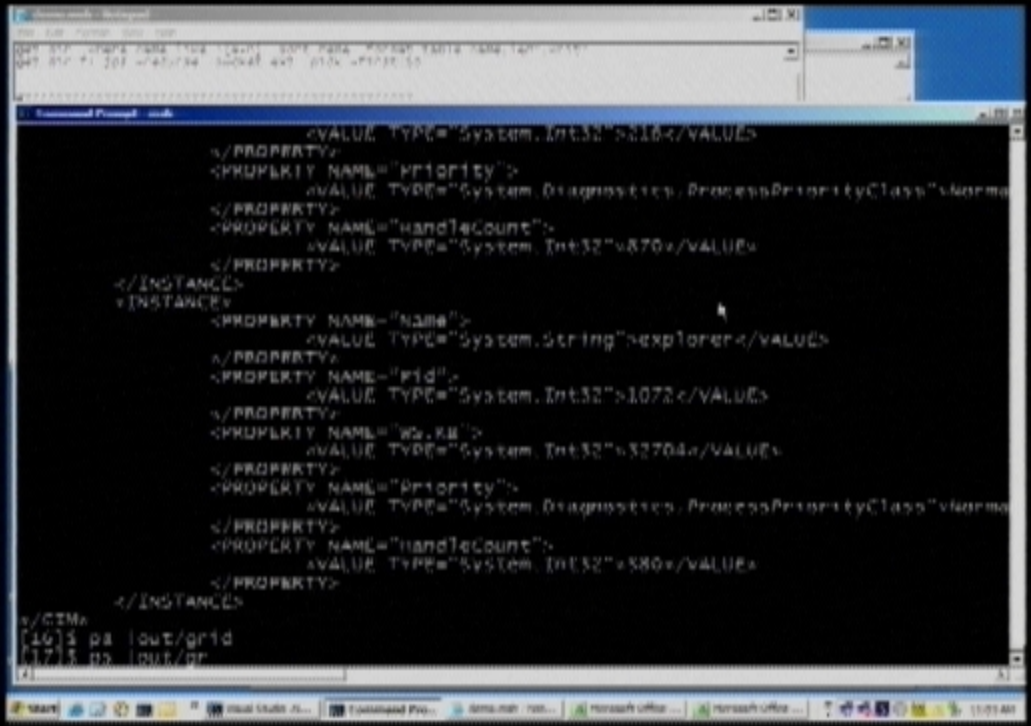

PROPERTY NAME="WS,KB"
VALUE TYPE="System.Int32"
PROPERTY NAME="Priority"
PROPERTY NAME="HandleCount"
INSTANCE
PROPERTY NAME="Name"
explorer
PROPERTY NAME="Pid"
PROPERTY NAME="WS,KB"
PROPERTY NAME="Priority"
PROPERTY NAME="HandleCount"
INSTANCE
CIM

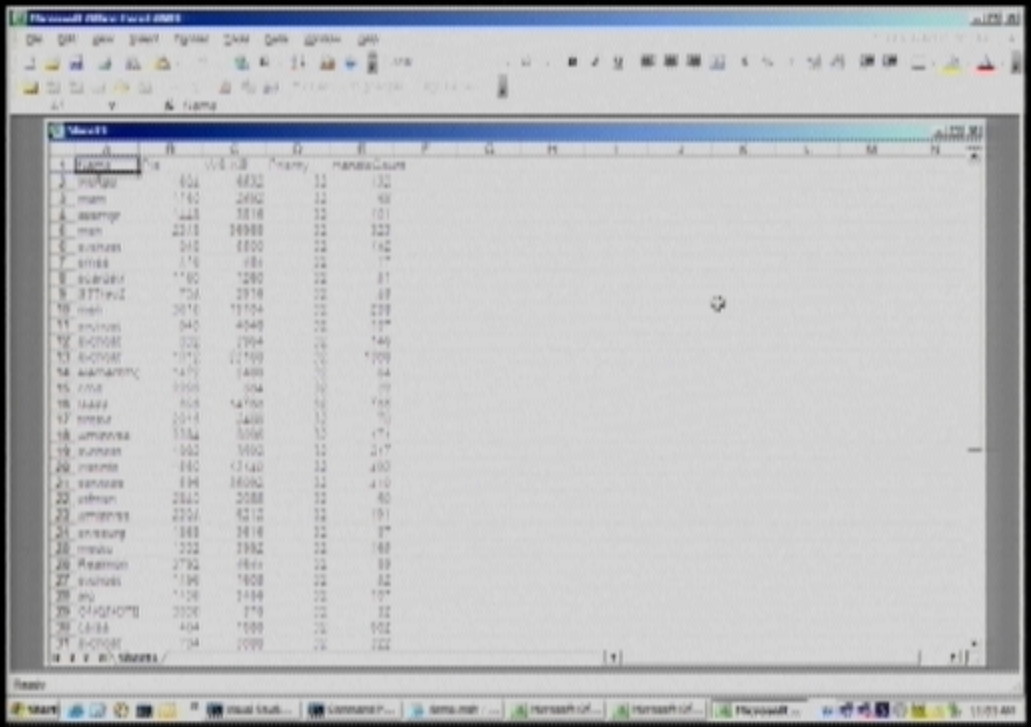


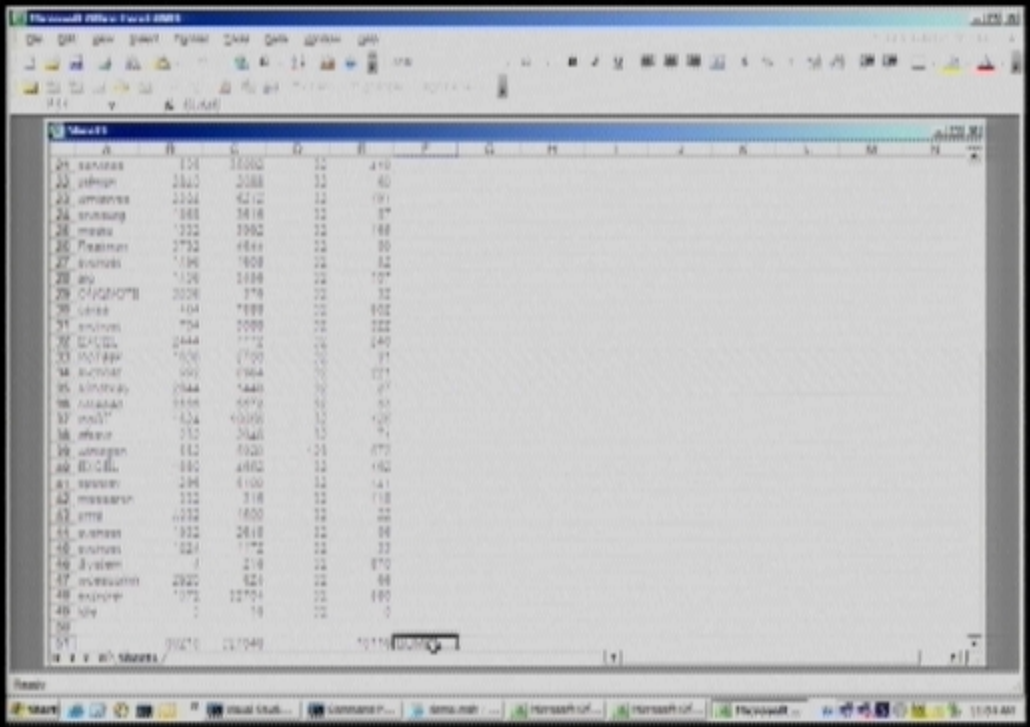

Results From:
Refresh
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$

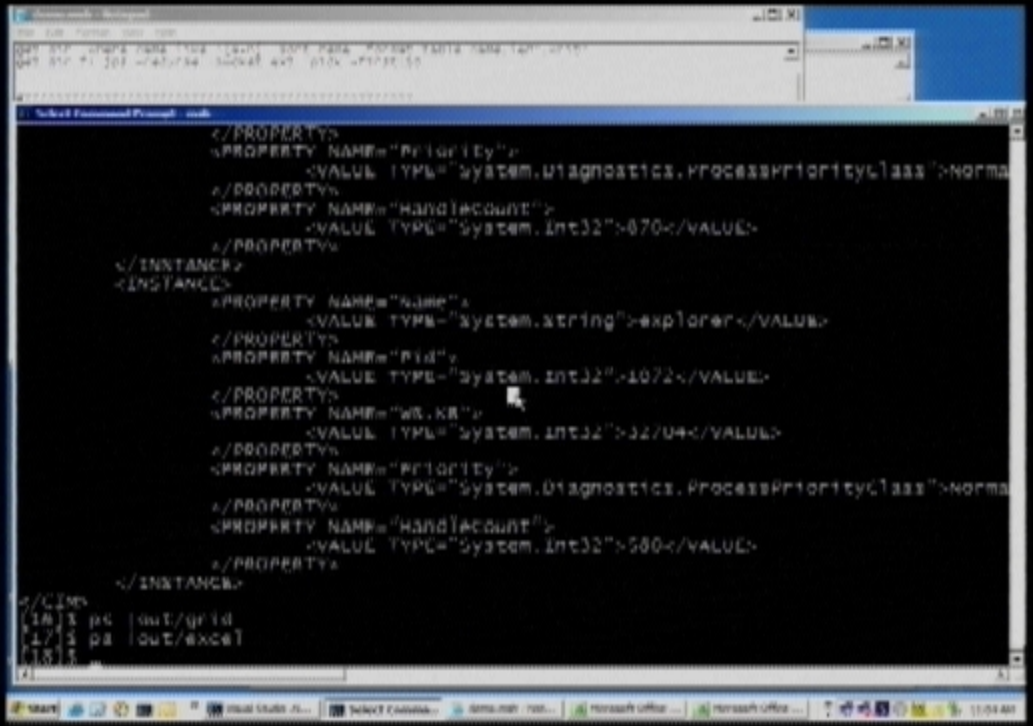


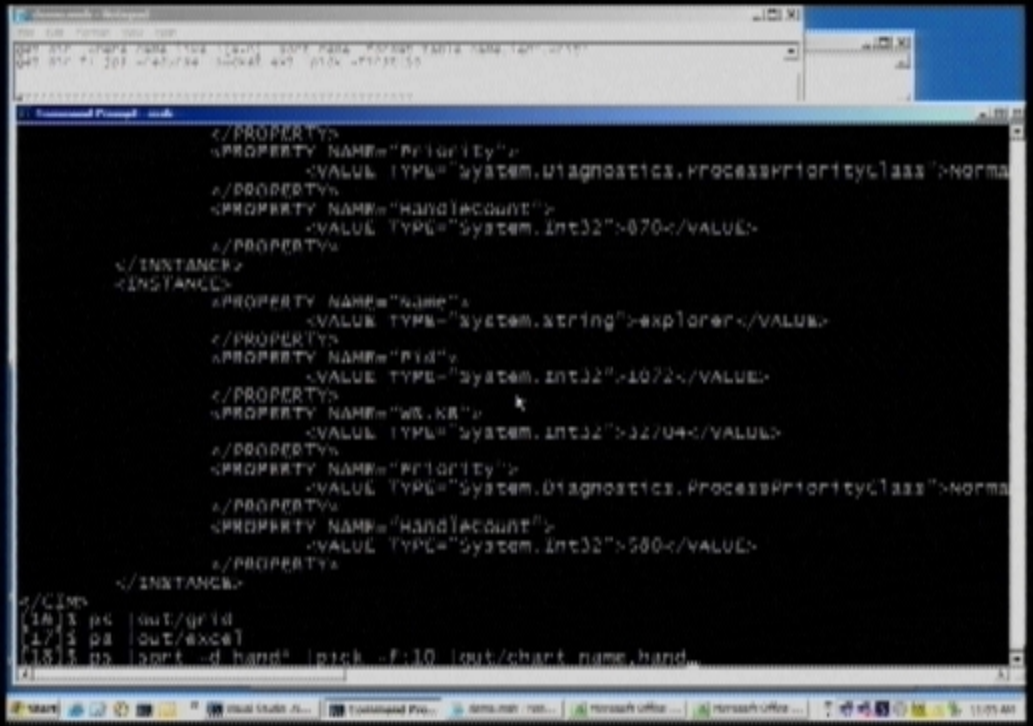


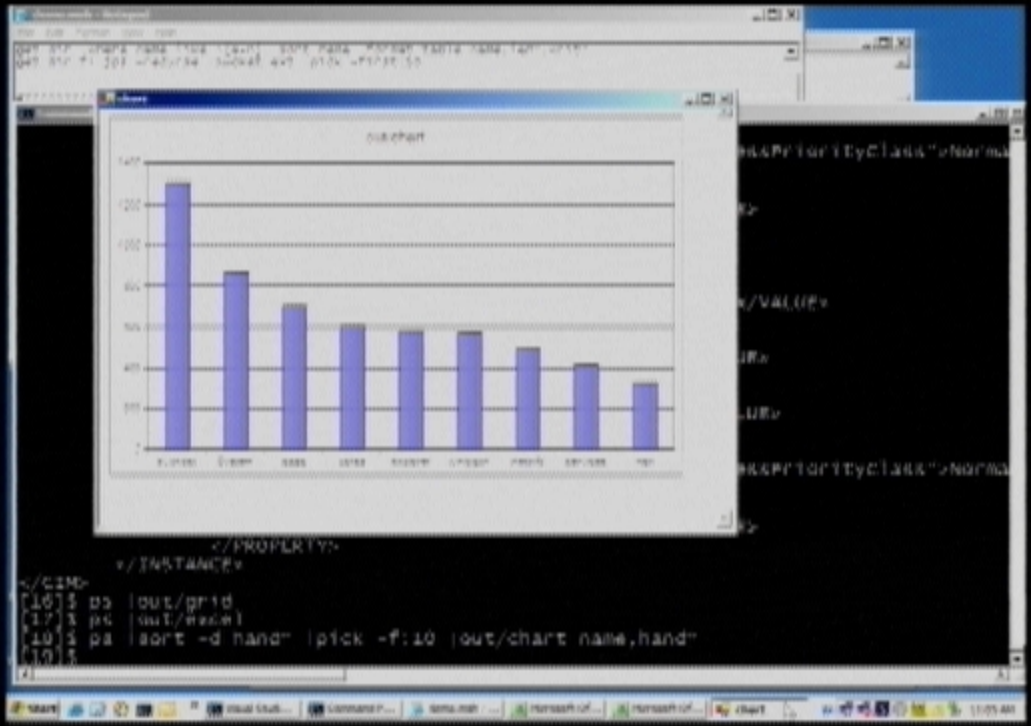

Command Prompt - cmd
<VALUE TYPE="System.Int32">316</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Normal
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">870</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">explorer</VALUE>
</PROPERTY>
<PROPERTY NAME="Pid">
<VALUE TYPE="System.Int32">1072</VALUE>
</PROPERTY>
<PROPERTY NAME="WS.KB">
<VALUE TYPE="System.Int32">52704</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Normal
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">580</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$ ps |out/gr

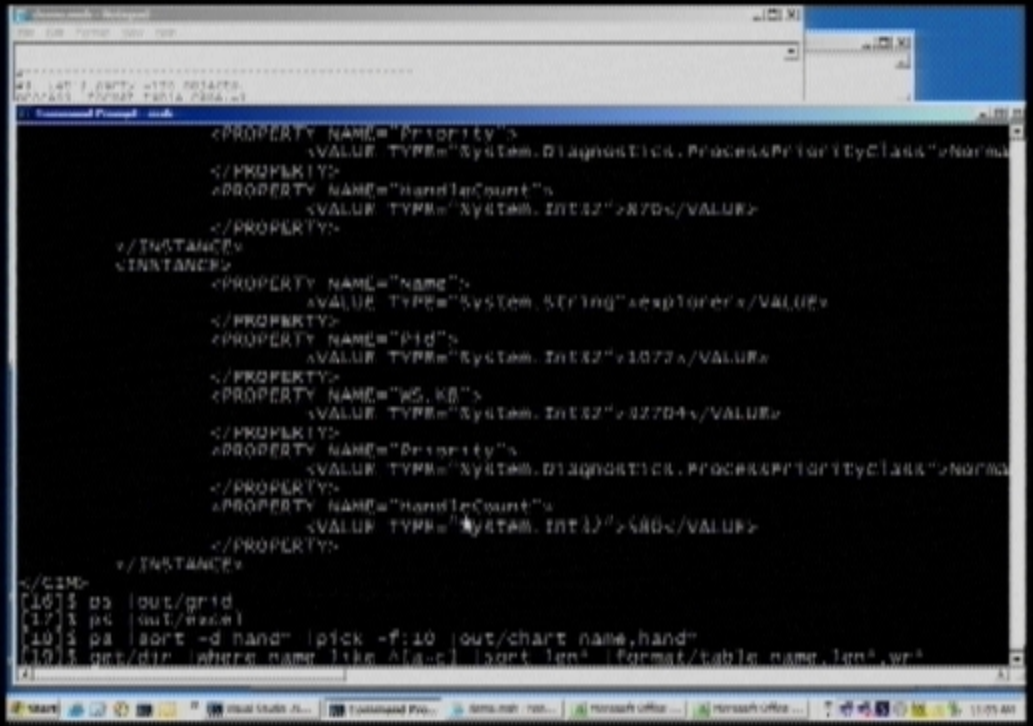


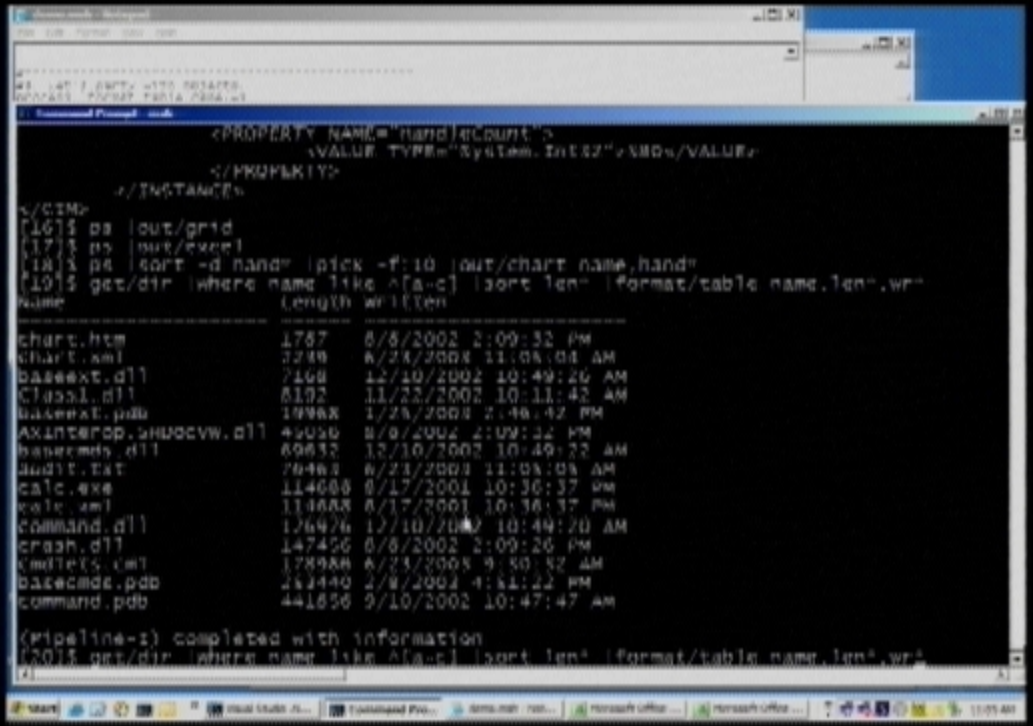


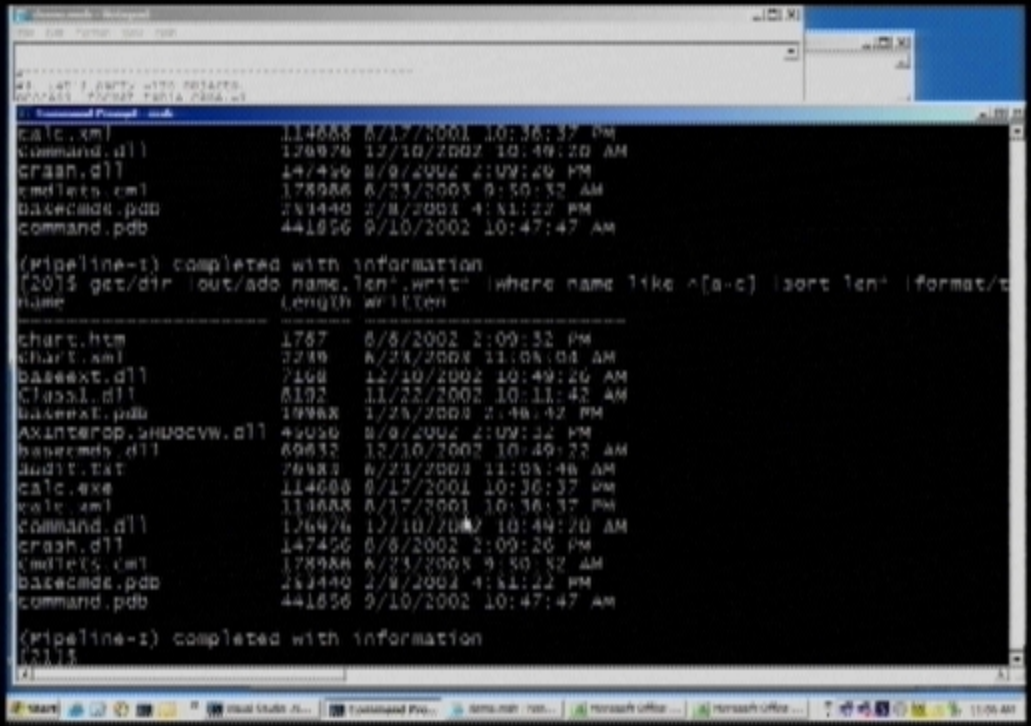

Select Command Prompt - ssh
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Norma
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">870</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">explorer</VALUE>
</PROPERTY>
<PROPERTY NAME="Pid">
<VALUE TYPE="System.Int32">1072</VALUE>
</PROPERTY>
<PROPERTY NAME="WS.KB">
<VALUE TYPE="System.Int32">32704</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Norma
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">580</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$ ps |out/excel
[18]$

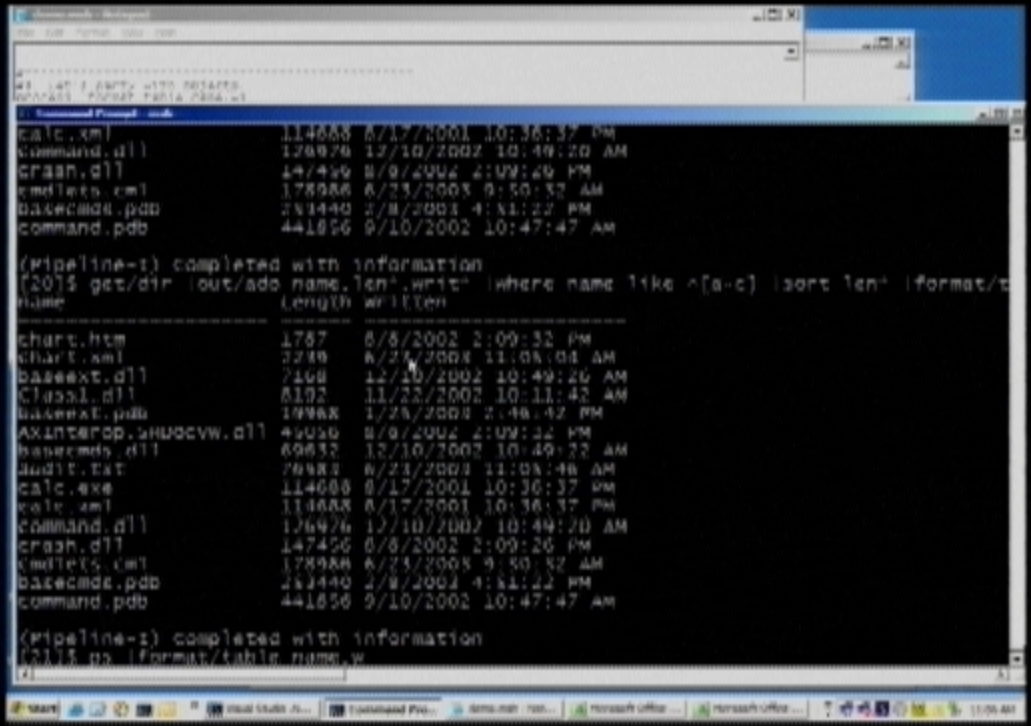

Command Prompt
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Norma
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">870</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">explorer</VALUE>
</PROPERTY>
<PROPERTY NAME="Pid">
<VALUE TYPE="System.Int32">1072</VALUE>
</PROPERTY>
<PROPERTY NAME="WS.KB">
<VALUE TYPE="System.Int32">32704</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Norma
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">580</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$ ps |out/excel
[18]$ ps |sort -d hand* |pick -f:10 |out/chart name,hand

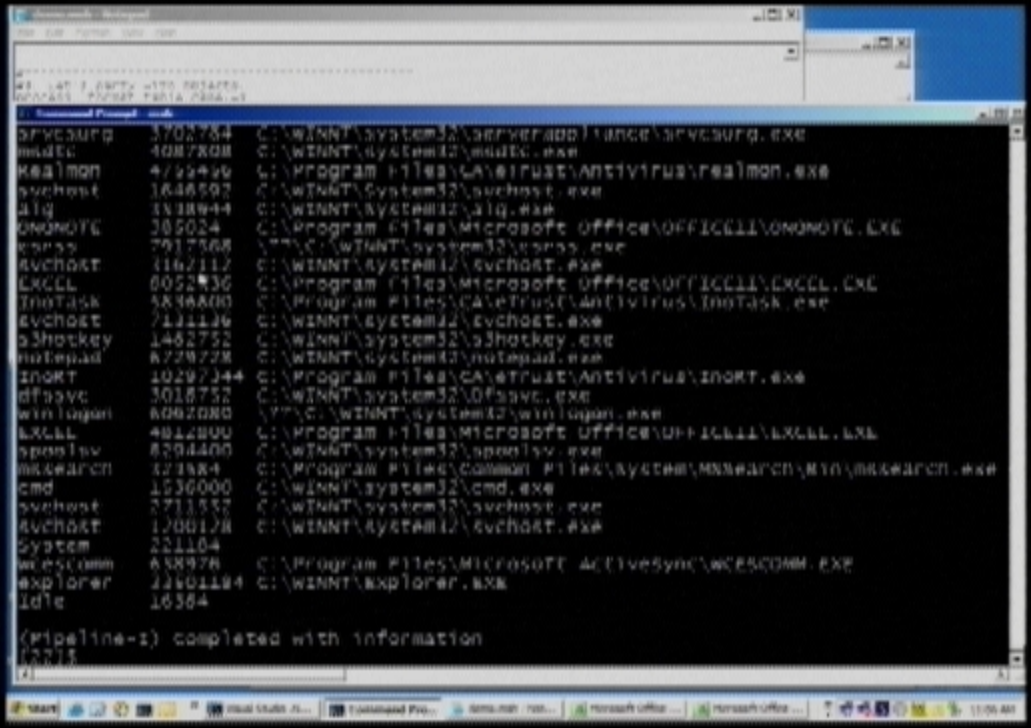

out/chart
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$ ps |out/excel
[18]$ ps |sort -d hand" |pick -f:10 |out/chart name,hand"
[19]$

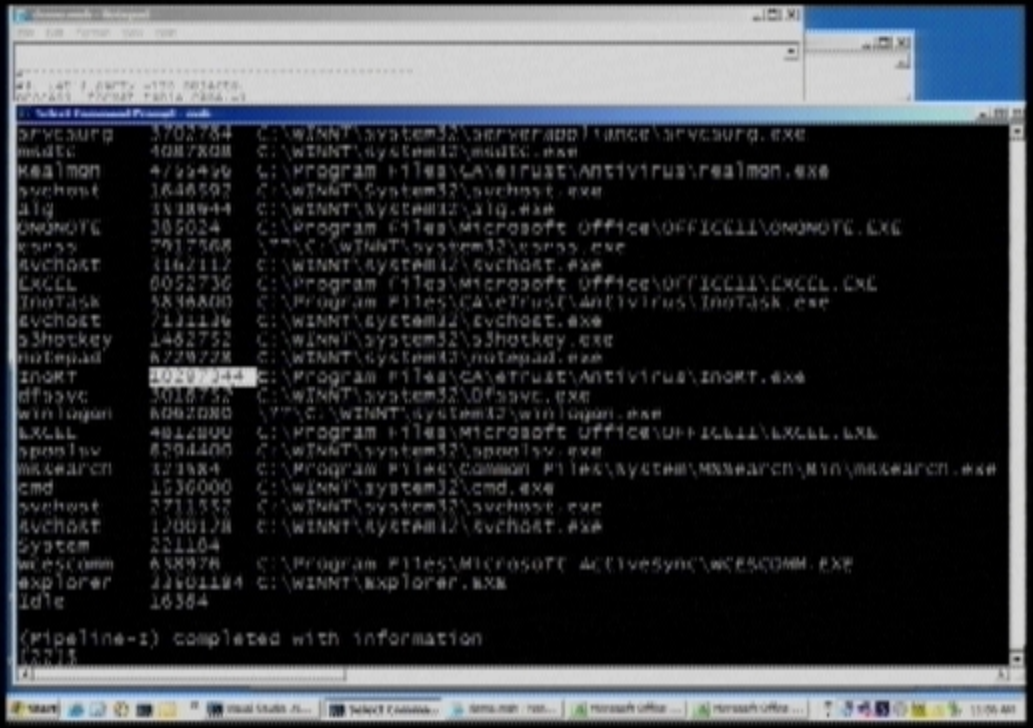

Command Prompt
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Normal
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">870</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">explorer</VALUE>
</PROPERTY>
<PROPERTY NAME="Pid">
<VALUE TYPE="System.Int32">1077</VALUE>
</PROPERTY>
<PROPERTY NAME="WS.KB">
<VALUE TYPE="System.Int32">82704</VALUE>
</PROPERTY>
<PROPERTY NAME="Priority">
<VALUE TYPE="System.Diagnostics.ProcessPriorityClass">Normal
</PROPERTY>
<PROPERTY NAME="HandleCount">
<VALUE TYPE="System.Int32">480</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$ ps |out/excel
[18]$ ps |sort -d name" |pick -f:10 |out/chart name,hand"
[19]$ gps/dir |where name like A[a-c] |sort len* |format/table name,len*,wr*

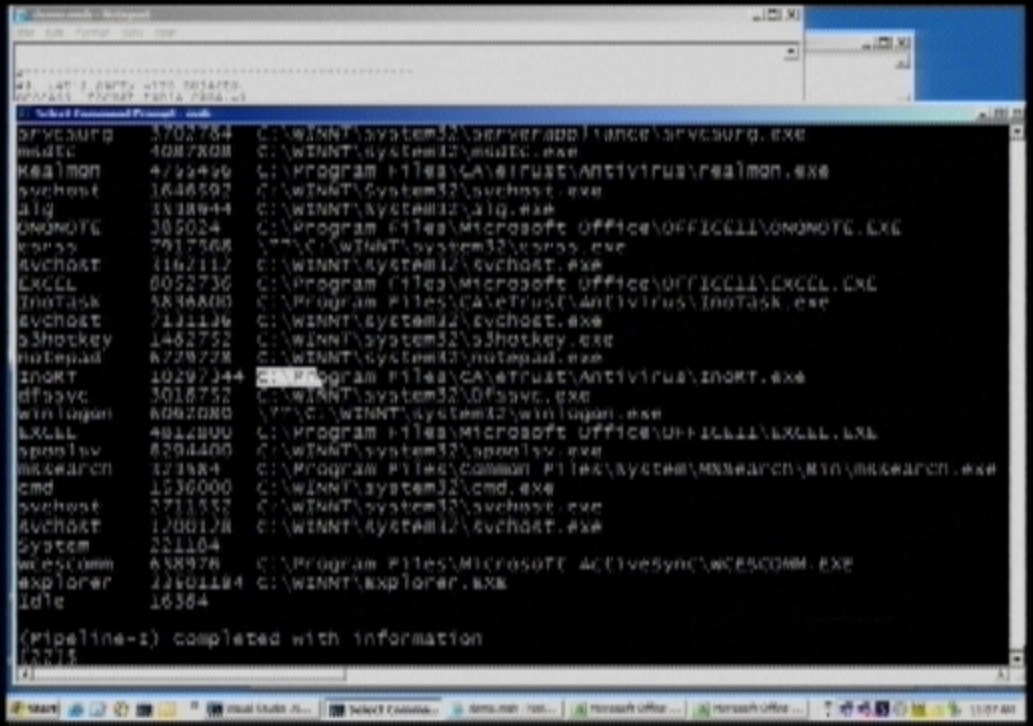

<PROPERTY NAME="nameHCount">
<VALUE TYPE="System.Int32">MD</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>
[16]$ ps |out/grid
[17]$ ps |out/excel
[18]$ ps |sort -d name |pick -f:10 |out/chart name,hand
[19]$ get/dir |where name like ^[a-c] |sort len |format/table name,len*,wr*
Name Length written
chart.htm 1787 8/8/2002 2:09:32 PM
chart.xml 3249 8/23/2005 11:05:04 AM
basexml.dll 7168 12/10/2002 10:49:26 AM
CTapsl.dll 8192 11/22/2002 10:11:42 AM
basexml.pdb 19968 1/25/2005 2:48:42 PM
AxInterop.SHDocVw.dll 46656 8/8/2002 2:09:32 PM
basecmds.dll 69632 12/10/2002 10:49:22 AM
audit.txt 70463 8/23/2005 11:05:05 AM
calc.exe 114688 8/17/2001 10:36:37 PM
calc.xml 114688 8/17/2001 10:36:37 PM
command.dll 126976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.xml 178986 8/23/2005 9:50:52 AM
basecmds.pdb 253440 2/8/2002 4:52:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(Pipeline-1) completed with information
[20]$ get/dir |where name like ^[a-c] |sort len |format/table name,len*,wr*

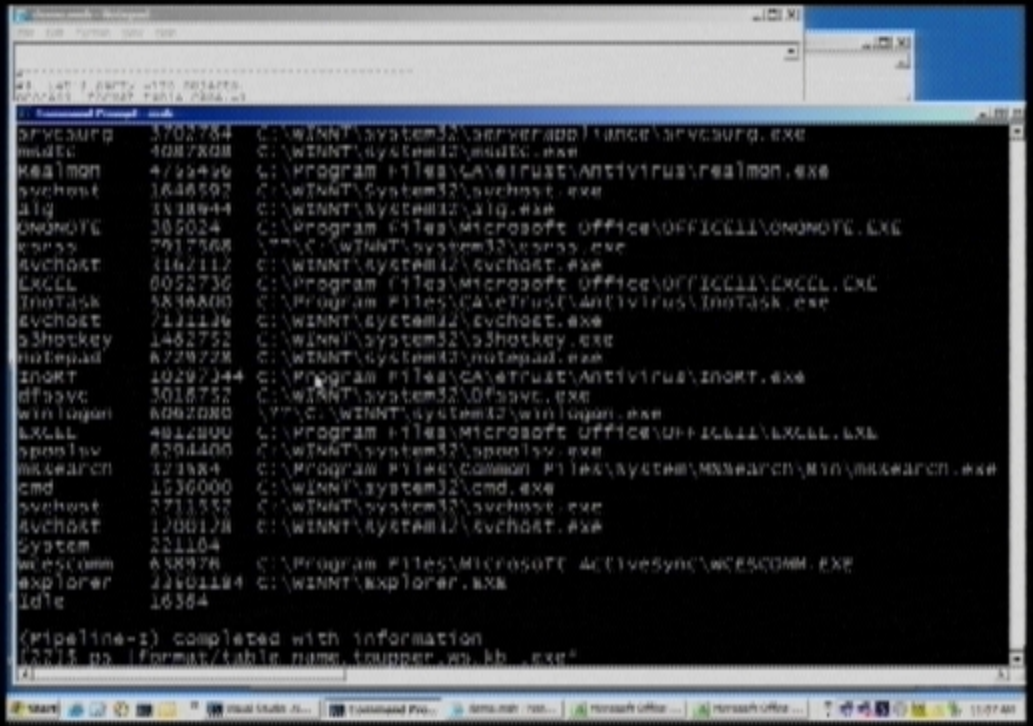

calc.xml 114688 8/17/2001 10:36:37 PM
command.dll 176976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.cml 178986 8/23/2005 9:50:52 AM
basecmds.pdb 253440 2/8/2004 4:51:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(pipeline-1) completed with information
[207] get/dir |out/ado name.len*.writ* |where name like ^[a-c] |sort len* |format/t
Name Length Written
chart.htm 1787 8/8/2002 2:09:32 PM
chart.xml 3249 8/23/2005 11:05:04 AM
baseext.dll 7168 12/10/2002 10:49:26 AM
CTest1.dll 8192 11/22/2002 10:11:42 AM
baseext.pdb 19968 1/25/2004 2:48:42 PM
AxInterop.SHDocVw.dll 46656 8/8/2002 2:09:32 PM
basecmds.dll 69632 12/10/2002 10:49:22 AM
audit.txt 70881 8/23/2005 11:05:46 AM
calc.exe 114688 8/17/2001 10:36:37 PM
calc.xml 114688 8/17/2001 10:36:37 PM
command.dll 176976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.cml 178986 8/23/2005 9:50:52 AM
basecmds.pdb 253440 2/8/2004 4:51:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(pipeline-1) completed with information

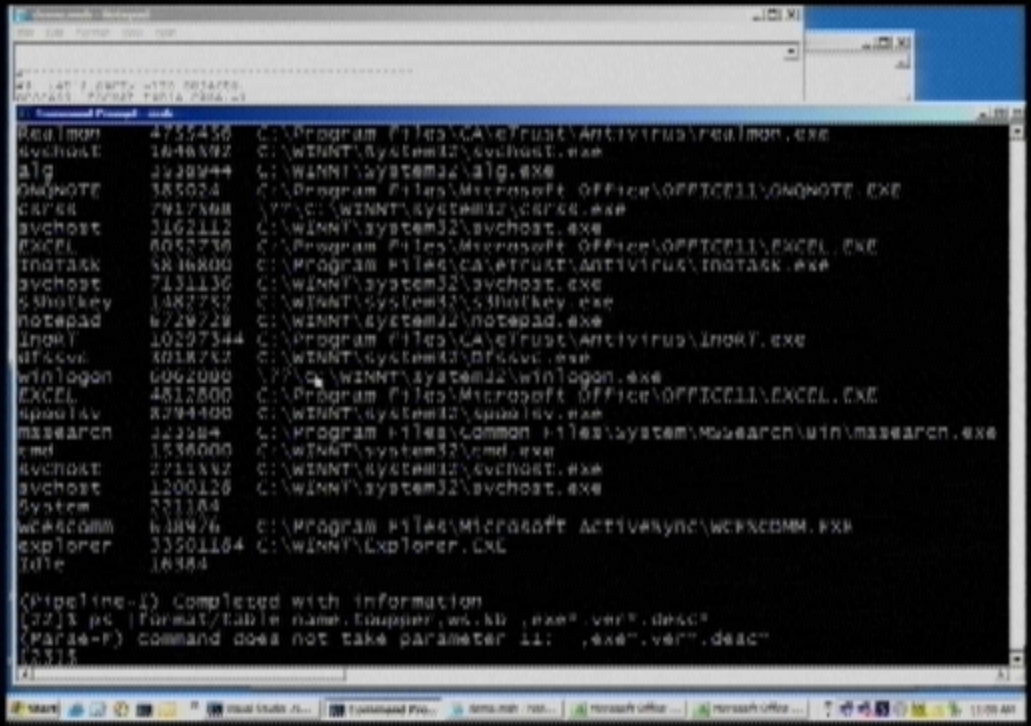

calc.xml 114688 8/17/2001 10:36:37 PM
Command.dll 126976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.cml 178986 8/23/2005 9:50:52 AM
basecmds.pdb 253440 2/8/2004 4:51:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(pipeline-1) completed with information
[20]$ get/dir |out/ado name.len*.writ* |where name like ^[a-c] |sort len* |format/t
name length written
chart.htm 1787 8/8/2002 2:09:32 PM
chart.xml 3249 8/23/2005 11:05:04 AM
baseext.dll 7168 12/10/2002 10:49:26 AM
CTpsxl.dll 8192 11/22/2002 10:11:42 AM
baseext.pdb 19968 1/25/2004 2:48:42 PM
AxInterop.SHDocVw.dll 46080 8/8/2002 2:09:32 PM
basecmds.dll 69632 12/10/2002 10:49:22 AM
audit.txt 78881 8/23/2005 11:05:48 AM
calc.exe 114688 8/17/2001 10:36:37 PM
calc.xml 114688 8/17/2001 10:36:37 PM
Command.dll 126976 12/10/2002 10:49:20 AM
crash.dll 147456 8/8/2002 2:09:26 PM
cmdlets.cml 178986 8/23/2005 9:50:52 AM
basecmds.pdb 253440 2/8/2004 4:51:22 PM
command.pdb 441856 9/10/2002 10:47:47 AM
(pipeline-1) completed with information
[21]$ ps |format/table name,w

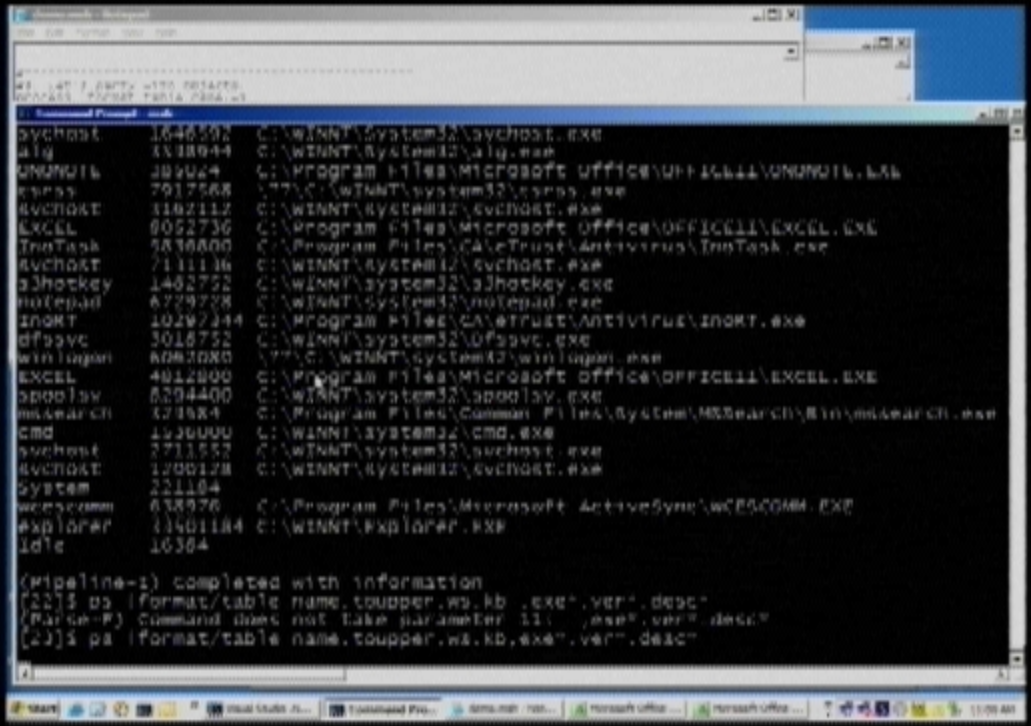

C:\Command Prompt - cmd
srvcsvrg 3702784 C:\WINNT\system32\servermanager\srvcsvrg.exe
msdtc 4087808 C:\WINNT\system32\msdtc.exe
realmon 4724416 C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost 1646592 C:\WINNT\System32\svchost.exe
alg 1138944 C:\WINNT\system32\alg.exe
ONQMOTE 385024 C:\Program Files\Microsoft Office\OFFICE11\ONQMOTE.EXE
csrss 7917568 C:\WINNT\system32\csrss.exe
svchost 4162112 C:\WINNT\system32\svchost.exe
EXCEL 8052736 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask 5496808 C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost 7111136 C:\WINNT\system32\svchost.exe
s3hotkey 1462752 C:\WINNT\system32\s3hotkey.exe
notepad 8720728 C:\WINNT\system32\notepad.exe
inoRT 10297344 C:\Program Files\CA\eTrust\Antivirus\inoRT.exe
dfssvc 3018752 C:\WINNT\system32\Dfssvc.exe
winlogon 6082080 C:\WINNT\system32\winlogon.exe
EXCEL 4012800 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv 8204800 C:\WINNT\system32\spoolsv.exe
mssearch 823584 C:\Program Files\Common Files\System\MSSearch\Bin\mssearch.exe
cmd 1536000 C:\WINNT\system32\cmd.exe
svchost 2711552 C:\WINNT\system32\svchost.exe
svchost 1200128 C:\WINNT\system32\svchost.exe
System 221184
wcescomm 65808 C:\Program Files\Microsoft ActiveSync\wcescomm.exe
explorer 11601184 C:\WINNT\explorer.exe
Idle 16384
(Pipeline-1) completed with information

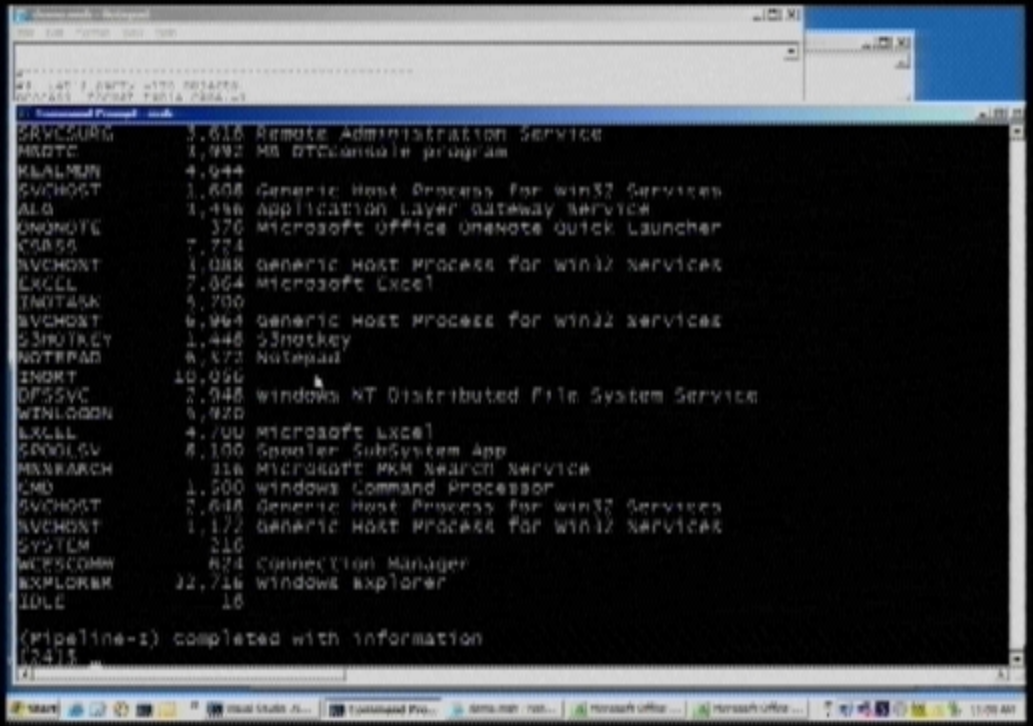

srvcsurg 3702784 C:\WINNT\system32\servermanager\srvcsurg.exe
msdtc 4087808 C:\WINNT\system32\msdtc.exe
realmon 4724420 C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost 1646592 C:\WINNT\System32\svchost.exe
alg 1318944 C:\WINNT\system32\alg.exe
ONENOTE 385024 C:\Program Files\Microsoft Office\OFFICE11\ONENOTE.EXE
csrss 7917568 C:\WINNT\system32\csrss.exe
svchost 1162112 C:\WINNT\system32\svchost.exe
EXCEL 8052736 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask 5496800 C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost 7331136 C:\WINNT\system32\svchost.exe
s3hotkey 1462752 C:\WINNT\system32\s3hotkey.exe
notepad 8778728 C:\WINNT\system32\notepad.exe
inoRT 10203744 C:\Program Files\CA\eTrust\Antivirus\inoRT.exe
dfssvc 3018752 C:\WINNT\system32\Dfssvc.exe
winlogon 6082080 C:\WINNT\system32\winlogon.exe
EXCEL 4812800 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv 8204800 C:\WINNT\system32\spoolsv.exe
mssearch 323584 C:\Program Files\Common Files\System\MSSearch\Bin\mssearch.exe
cmd 1536000 C:\WINNT\system32\cmd.exe
svchost 2711552 C:\WINNT\system32\svchost.exe
svchost 1200128 C:\WINNT\system32\svchost.exe
System 221184
wcescomm 65976 C:\Program Files\Microsoft ActiveSync\wCESCOMM.EXE
explorer 21601184 C:\WINNT\explorer.exe
Idle 16384
(Pipeline-1) completed with information

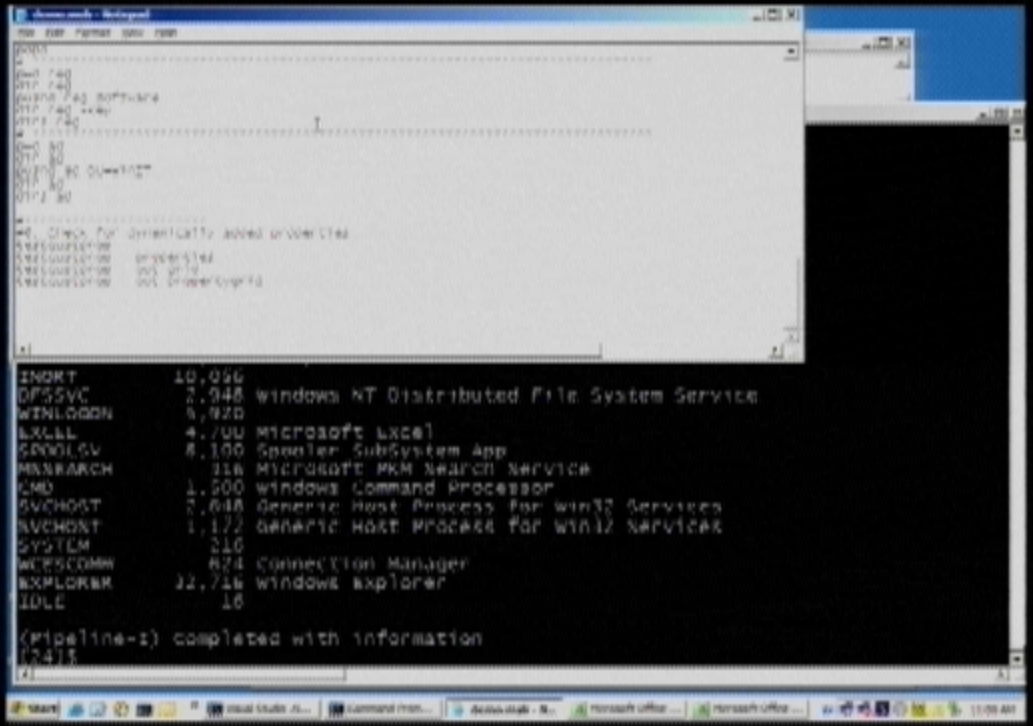

srvcsurg 3702784 C:\WINNT\system32\servermon\ance\srvcsurg.exe
msdtc 4087808 C:\WINNT\system32\msdtc.exe
realmon 4764496 C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost 1646592 C:\WINNT\System32\svchost.exe
alg 1138944 C:\WINNT\system32\alg.exe
ONENOTE 385024 C:\Program Files\Microsoft Office\OFFICE11\ONENOTE.EXE
csrss 7917568 \??\C:\WINNT\system32\csrss.exe
svchost 1162112 C:\WINNT\system32\svchost.exe
EXCEL 8052736 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask 5496808 C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost 7331136 C:\WINNT\system32\svchost.exe
s3hotkey 1462752 C:\WINNT\system32\s3hotkey.exe
notepad 6778728 C:\WINNT\system32\notepad.exe
inoRT 10297344 C:\Program Files\CA\eTrust\Antivirus\inoRT.exe
dfssvc 3018752 C:\WINNT\system32\Dfssvc.exe
winlogon 6082080 \??\C:\WINNT\system32\winlogon.exe
EXCEL 4812800 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv 8204800 C:\WINNT\system32\spoolsv.exe
mssearch 323584 C:\Program Files\Common Files\System\MSSearch\Bin\mssearch.exe
cmd 1536000 C:\WINNT\system32\cmd.exe
svchost 2711552 C:\WINNT\system32\svchost.exe
avchost 1200128 C:\WINNT\system32\avchost.exe
System 221184
wcescomm 65976 C:\Program Files\Microsoft ActiveSync\wCESCOMM.EXE
explorer 11601184 C:\WINNT\explorer.exe
Idle 16384
(Pipeline-1) completed with information

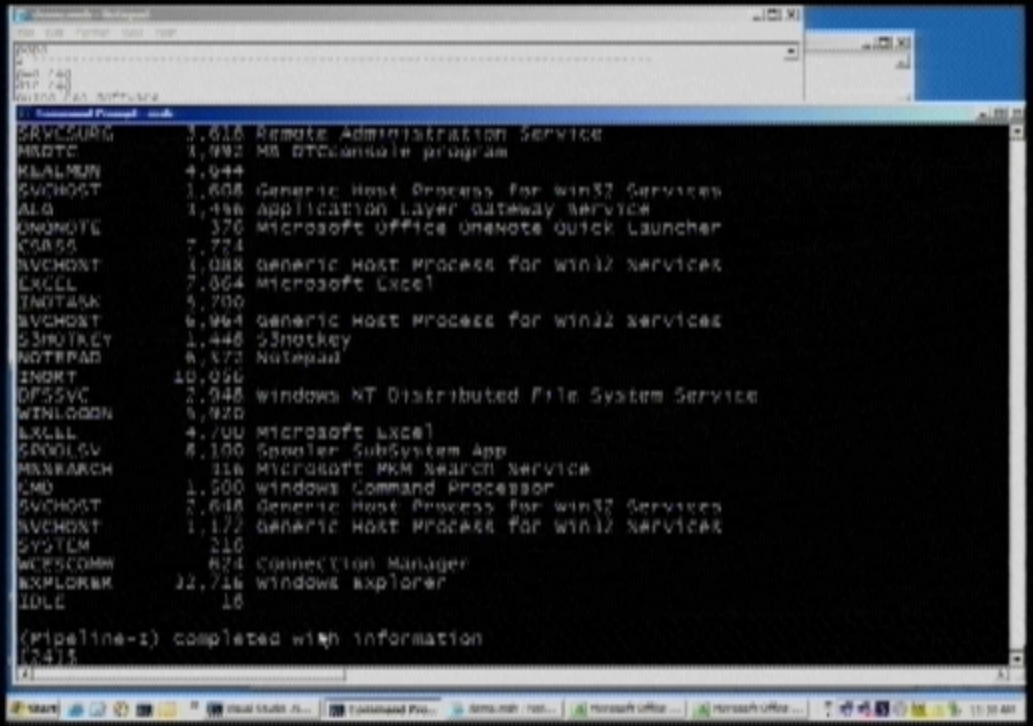

srvcsurg 3702764 C:\WINNT\system32\server.app|ance\srvcsurg.exe
msdtc 4087608 C:\WINNT\system32\msdtc.exe
realmon 4764476 C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost 1646592 C:\WINNT\System32\svchost.exe
alg 1138944 C:\WINNT\system32\alg.exe
ONQMOTE 385024 C:\Program Files\Microsoft Office\OFFICE11\ONQMOTE.EXE
csrss 7917568 \??\C:\WINNT\system32\csrss.exe
svchost 4162112 C:\WINNT\system32\svchost.exe
EXCEL 8052736 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask 5496808 C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost 7111136 C:\WINNT\system32\svchost.exe
s3hotkey 1462752 C:\WINNT\system32\s3hotkey.exe
notepad 872972 C:\WINNT\system32\notepad.exe
inoRT 10297344 C:\Program Files\CA\eTrust\Antivirus\inoRT.exe
dfssvc 3018752 C:\WINNT\system32\Dfssvc.exe
winlogon 6062080 \??\C:\WINNT\system32\winlogon.exe
EXCEL 4812800 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv 8204800 C:\WINNT\system32\spoolsv.exe
mssearch 323584 C:\Program Files\Common Files\System\MSSearch\Bin\mssearch.exe
cmd 1536000 C:\WINNT\system32\cmd.exe
svchost 2711552 C:\WINNT\system32\svchost.exe
svchost 1200128 C:\WINNT\system32\svchost.exe
System 221184
wcescomm 65976 C:\Program Files\Microsoft ActiveSync\wCESCOMM.EXE
explorer 21601184 C:\WINNT\explorer.exe
Idle 16384
(Pipeline-1) completed with information

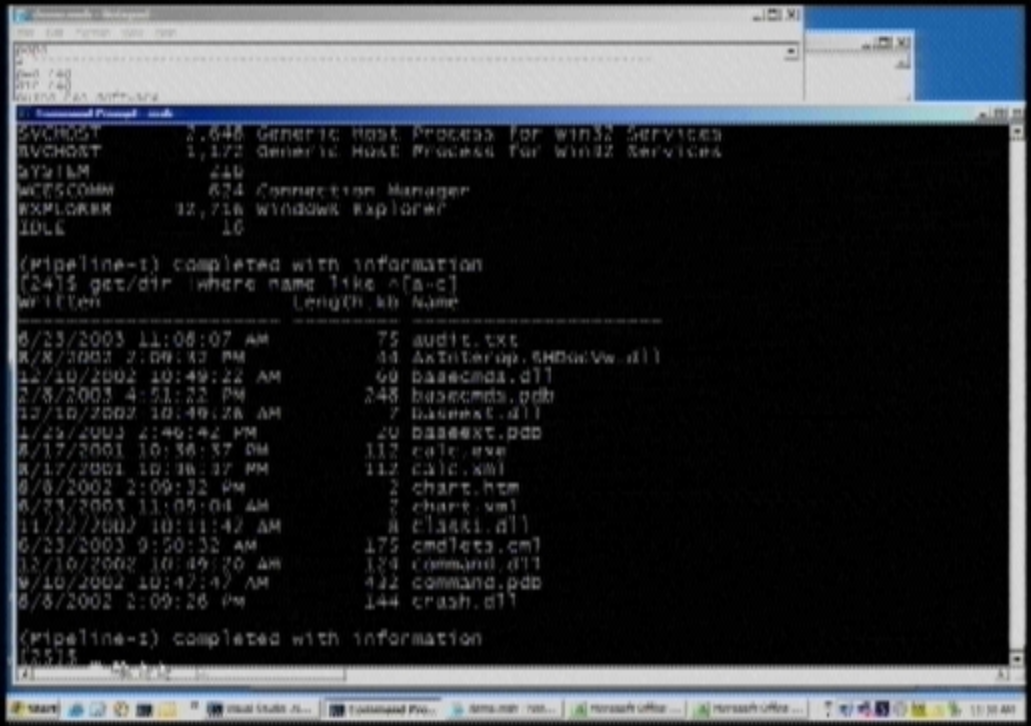

Realmon 2752456 C:\Program Files\CA\eTrust\Antivirus\realmon.exe
svchost 1048592 C:\WINNT\System32\svchost.exe
alg 2228944 C:\WINNT\system32\alg.exe
ONENOTE 185024 C:\Program Files\Microsoft Office\OFFICE11\ONENOTE.EXE
csrss 7917568 \??\C:\WINNT\system32\csrss.exe
svchost 3162112 C:\WINNT\system32\svchost.exe
EXCEL 8065760 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask 5816800 C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost 7131136 C:\WINNT\system32\svchost.exe
sShotkey 1482752 C:\WINNT\system32\sShotkey.exe
notepad 6729728 C:\WINNT\system32\notepad.exe
InoRT 10297344 C:\Program Files\CA\eTrust\Antivirus\InoRT.exe
nfsvc 5918752 C:\WINNT\system32\nfsvc.exe
winlogon 6062080 \??\C:\WINNT\system32\winlogon.exe
EXCEL 4812800 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv 8794400 C:\WINNT\system32\spoolsv.exe
msseacrn 323584 C:\Program Files\Common Files\System\Msseacrn\win\msseacrn.exe
cmd 1536000 C:\WINNT\system32\cmd.exe
svchost 2711552 C:\WINNT\system32\svchost.exe
svchost 1200128 C:\WINNT\system32\svchost.exe
System 221184
wcescomm 618976 C:\Program Files\Microsoft ActiveSync\wcescomm.exe
explorer 33501184 C:\WINNT\Explorer.EXE
Idle 16384
(Pipeline-1) Completed with information
[22]% ps |format-table name,Dapper,ws,kb ,exe",ver",desc"
(Parse-F) command does not take parameter 11: ,exe",ver",desc"

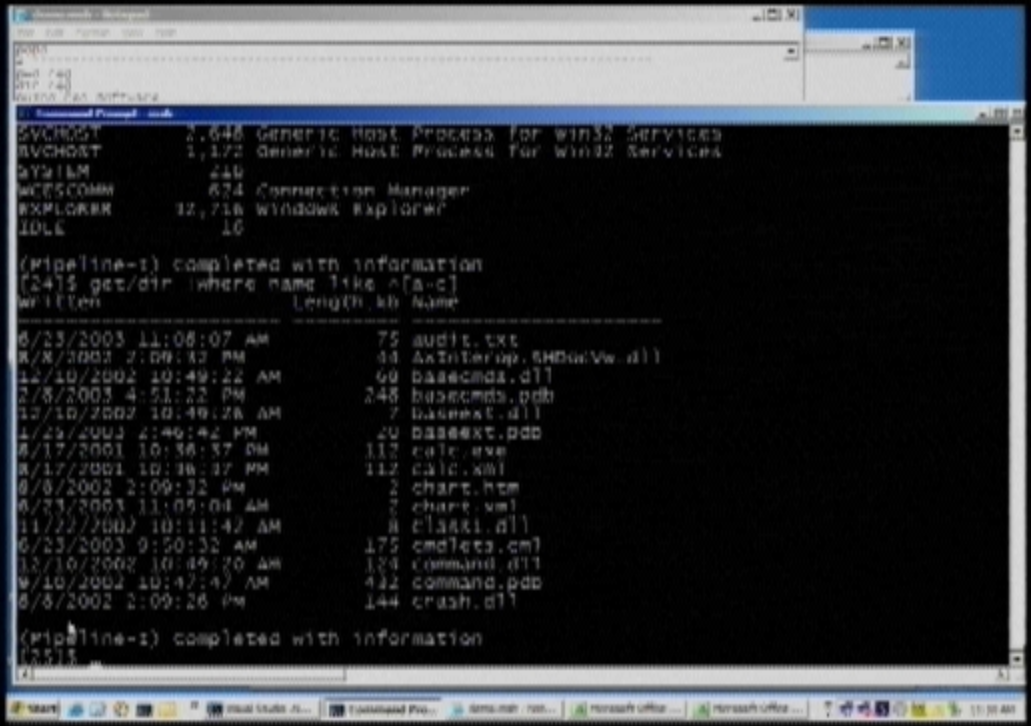

svchost 1040504 C:\WINNT\system32\svchost.exe
alg 1138944 C:\WINNT\System32\alg.exe
UNUNU16 280624 C:\Program Files\Microsoft Office\OFFICE11\UNUNU16.EXE
csrss 7917568 C:\??\C:\WINNT\system32\csrss.exe
svchost 1102112 C:\WINNT\system32\svchost.exe
EXCEL 8052736 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
InoTask 5816800 C:\Program Files\CA\eTrust\Antivirus\InoTask.exe
svchost 7111136 C:\WINNT\system32\svchost.exe
ajhotkey 1402752 C:\WINNT\system32\ajhotkey.exe
notepad 6779736 C:\WINNT\system32\notepad.exe
inoRT 10292344 C:\Program Files\CA\eTrust\Antivirus\inoRT.exe
dfssvc 3018752 C:\WINNT\system32\Dfssvc.exe
winlogon 6082080 \??\C:\WINNT\system32\winlogon.exe
EXCEL 4012800 C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE
spoolsv 8204400 C:\WINNT\system32\spoolsv.exe
msmsgrch 978584 C:\Program Files\Common Files\System\MSSearch\Bin\msmsgrch.exe
cmd 1536000 C:\WINNT\system32\cmd.exe
svchost 2711552 C:\WINNT\system32\svchost.exe
svchost 1700128 C:\WINNT\system32\svchost.exe
System 221184
wcescomm 638976 C:\Program Files\Microsoft ActiveSync\wCESCOMM.EXE
explorer 11401184 C:\WINNT\Explorer.EXE
Idle 16384
(Pipeline-1) completed with information
[22]$ ps |format/table name.toupper.ws.kb ,exe",ver",desc"
(Parse-P) Command does not take parameter 11: ,exe",ver",desc"
[23]$ ps |format/table name.toupper.ws.kb,exe",ver",desc"

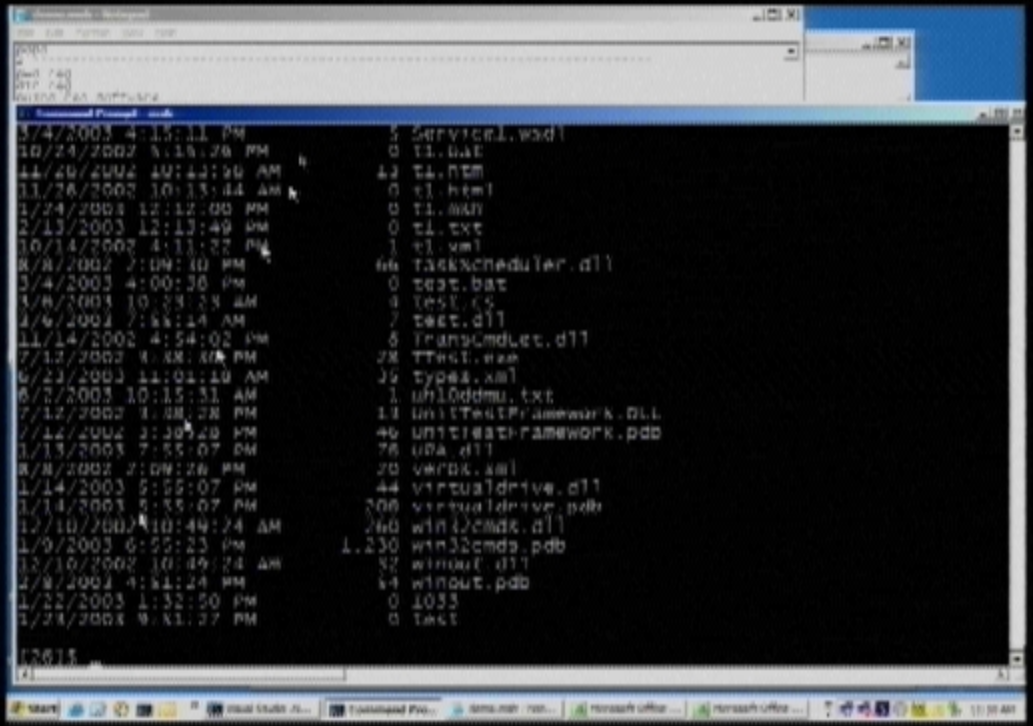

SRVCSURG 3,616 Remote Administration Service
MSDTC 1,892 MS DTC Console program
MSALMGR 4,044
SVCHOST 1,608 Generic Host Process for Win32 Services
ALG 3,496 Application Layer Gateway Service
ONENOTE 376 Microsoft Office OneNote Quick Launcher
CSRSS 7,774
SVCHOST 1,088 Generic Host Process for Win32 Services
EXCEL 7,864 Microsoft Excel
TNOTARK 5,700
SVCHOST 6,964 Generic Host Process for Win32 Services
S3NOTKEY 1,448 S3notkey
NOTEPAD 6,572 Notepad
INORT 10,056
DFSSVC 2,048 Windows NT Distributed File System Service
WINLOGON 5,020
EXCEL 4,700 Microsoft Excel
SPOOLSV 8,100 Spooler SubSystem App
MSSEARCH 316 Microsoft MKM Search Service
CMD 1,500 Windows Command Processor
SVCHOST 2,648 Generic Host Process for Win32 Services
SVCHOST 1,172 Generic Host Process for Win32 Services
SYSTEM 216
WCESCOMM 872 Connection Manager
EXPLORER 32,716 Windows Explorer
IDLE 16
(Pipeline-1) completed with information

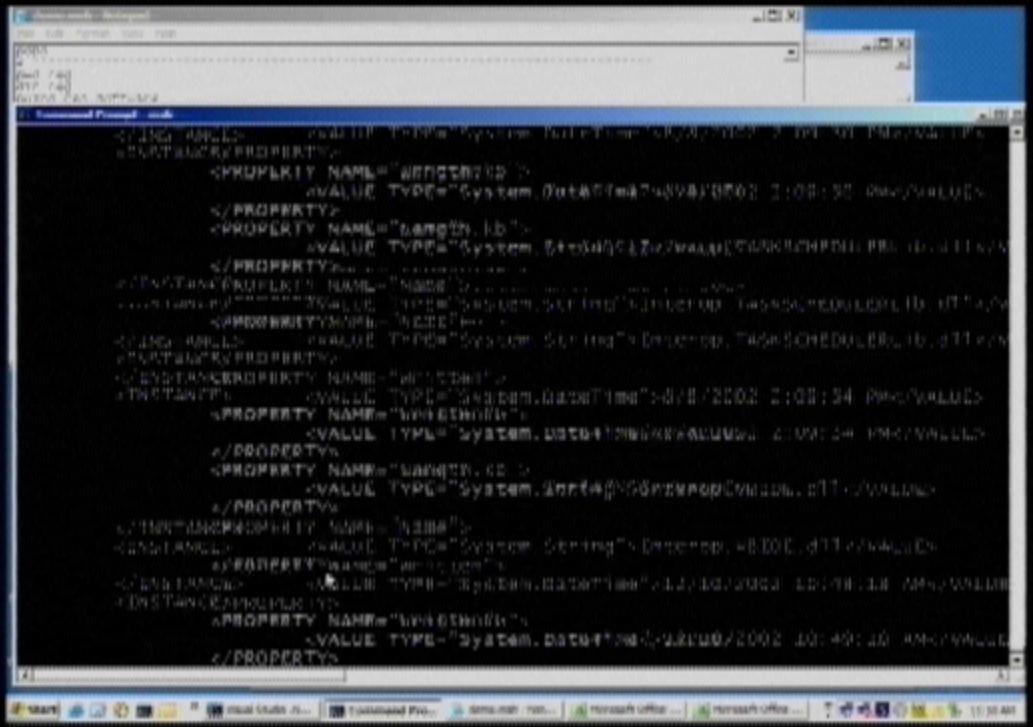

INORT 10,056
DFSSVC 2,048 Windows NT Distributed File System Service
WINLOGON 9,920
EXCEL 4,700 Microsoft Excel
SPOOLSV 8,100 Spooler SubSystem App
MSSEARCH 316 Microsoft MKM Search Service
CMD 1,300 Windows Command Processor
SVCHOST 2,048 Generic Host Process for Win32 Services
SVCHOST 1,172 Generic Host Process for Win32 Services
SYSTEM 216
WCESCOMM 824 Connection Manager
EXPLORER 32,716 Windows Explorer
IDLE 16
(Pipeline-1) completed with information

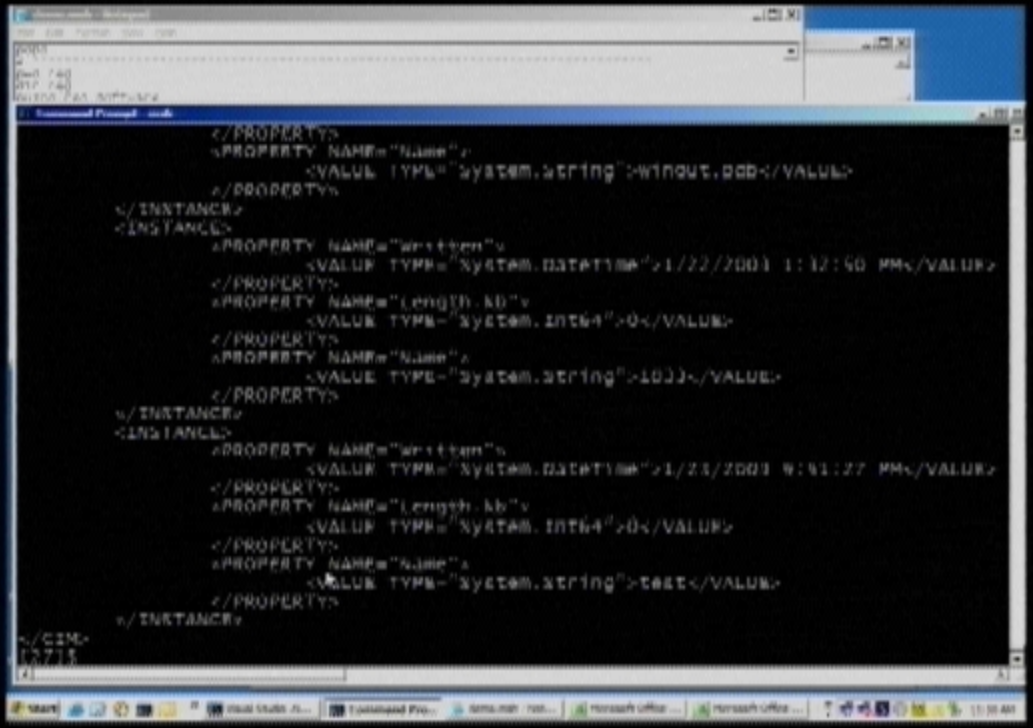

SRVCSURG 3,616 Remote Administration Service
MSDTC 1,892 MS DTC Console program
KEALMUN 4,044
SVCHOST 1,608 Generic Host Process for Win32 Services
ALG 1,496 Application Layer Gateway Service
ONENOTE 376 Microsoft Office OneNote Quick Launcher
CSRSS 7,774
SVCHOST 1,088 Generic Host Process for Win32 Services
EXCEL 7,864 Microsoft Excel
TASKMGR 5,700
SVCHOST 6,964 Generic Host Process for Win32 Services
S3HOTKEY 1,448 S3 Hotkey
NOTEPAD 6,572 Notepad
INORT 10,056
DFSSVC 2,048 Windows NT Distributed File System Service
WINLOGON 5,920
EXCEL 4,700 Microsoft Excel
SPOOLSV 8,100 Spooler SubSystem App
MSSEARCH 116 Microsoft MKM Search Service
CMD 1,500 Windows Command Processor
SVCHOST 2,648 Generic Host Process for Win32 Services
SVCHOST 1,172 Generic Host Process for Win32 Services
SYSTEM 216
WCESCOMM 872 Connection Manager
EXPLORER 22,716 Windows Explorer
IDLE 16
(Pipeline-1) completed with information

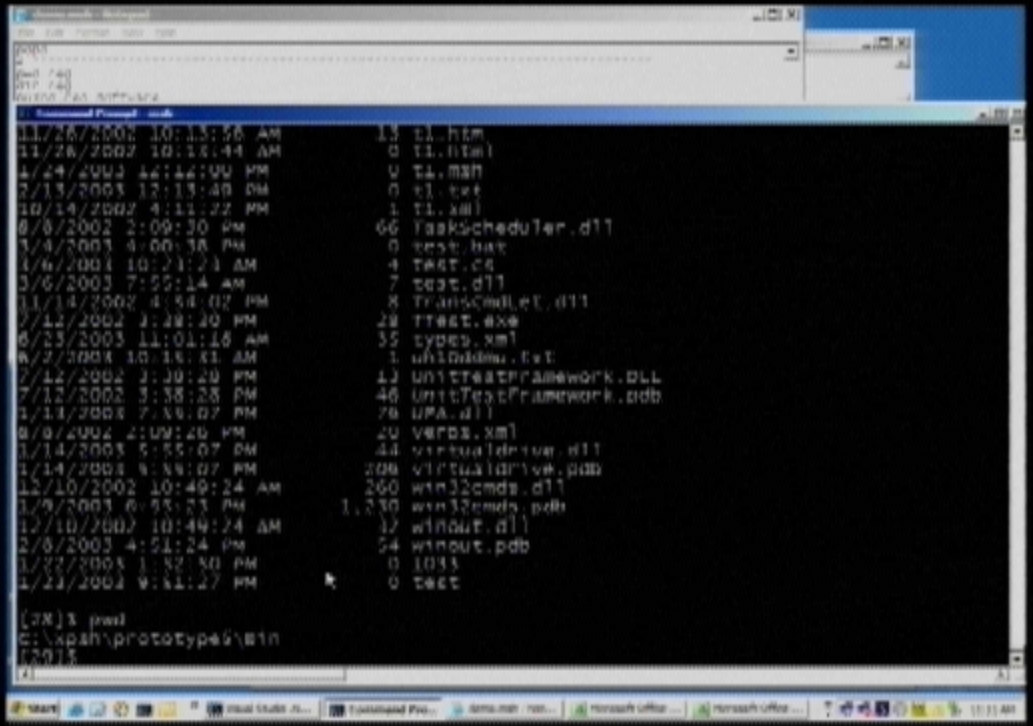

SVCHOST 2,648 Generic Host Process for Win32 Services
SVCHOST 1,172 Generic Host Process for Win32 Services
SYSTEM 220
WCESCOMM 872 Connection Manager
EXPLORER 12,716 Windows Explorer
IDLE 16
(Pipeline-1) completed with information
[241]$ get/dir -where name like ^[a-c]
Written Length,kb Name
6/23/2003 11:08:07 AM 75 audit.txt
12/10/2002 10:49:22 AM 60 basecmds.dll
2/8/2003 4:51:22 PM 248 basecmds.pdb
12/10/2002 10:49:26 AM 7 baseext.dll
1/23/2003 2:46:42 PM 20 baseext.pdb
8/17/2001 10:36:57 PM 112 calc.exe
8/17/2001 10:36:37 PM 112 calc.xml
6/8/2002 2:09:32 PM 2 chart.htm
6/23/2003 11:05:04 AM 7 chart.xml
11/22/2002 10:11:42 AM 8 clsasi.dll
6/23/2003 9:50:32 AM 175 cmdlets.cml
12/10/2002 10:49:20 AM 124 command.dll
9/10/2002 10:47:47 AM 432 command.pdb
6/8/2002 2:09:26 PM 144 crash.dll
(Pipeline-1) completed with information

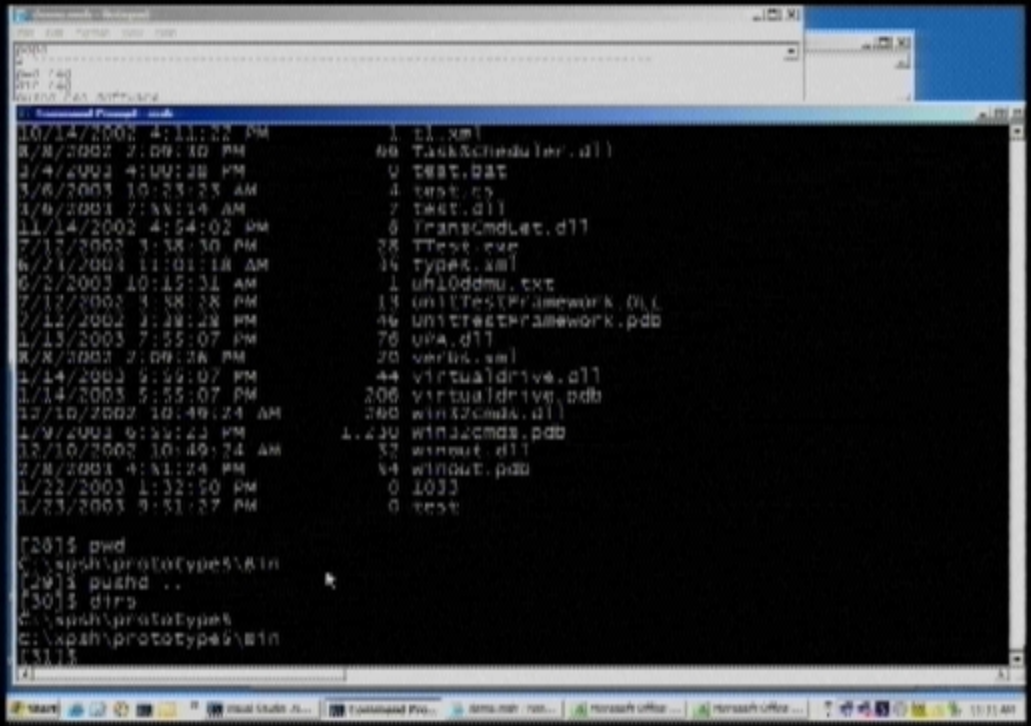

SVCHOST 2,648 Generic Host Process for Win32 Services
SVCHOST 1,172 Generic Host Process for Win32 Services
SYSTEM 240
WCESCOMM 872 Connection Manager
EXPLORER 12,716 Windows Explorer
IDLE 16
(Pipeline-1) completed with information
[241]$ get/dir |where name like ^[a-c]
Written Length,kb Name
6/23/2003 11:08:07 AM 75 audit.txt
12/10/2002 10:49:22 AM 60 basecmds.dll
2/8/2003 4:51:22 PM 248 basecmds.pdb
12/10/2002 10:49:26 AM 7 baseext.dll
6/17/2001 10:36:57 PM 112 calc.exe
6/8/2002 2:09:32 PM 2 chart.htm
6/23/2003 11:05:04 AM 2 chart.xml
11/22/2002 10:11:42 AM 8 clsAri.dll
6/23/2003 9:50:32 AM 175 cmdlets.cml
12/10/2002 10:49:20 AM 124 command.dll
9/10/2002 10:42:42 AM 432 command.pdb
6/8/2002 2:09:26 PM 144 crush.dll
(Pipeline-1) completed with information

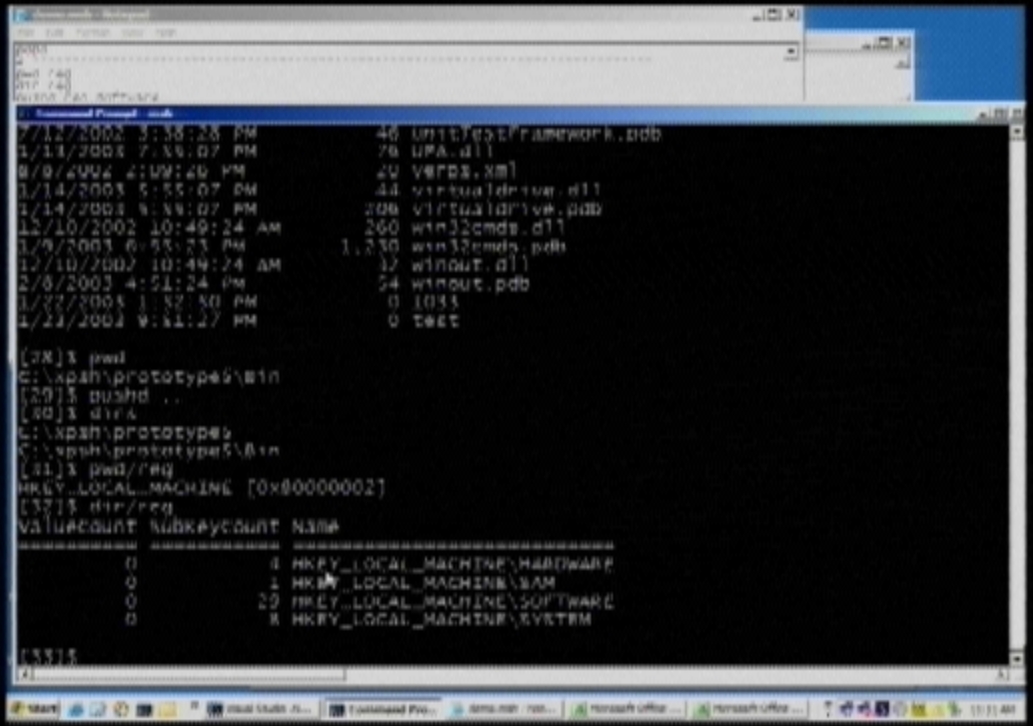

Command Prompt - cmd
5/4/2003 4:15:11 PM 5 Service1.wsdl
10/24/2002 5:16:26 PM 0 t1.out
11/20/2002 10:12:50 AM 12 t1.ntm
11/26/2002 10:15:44 AM 0 t1.html
1/24/2003 12:12:00 PM 0 t1.man
2/13/2003 12:13:49 PM 0 t1.txt
10/14/2002 4:11:27 PM 1 t1.xml
8/8/2002 7:00:10 PM 66 taskxcheduler.dll
5/4/2003 4:00:36 PM 0 test.bat
5/8/2003 10:29:58 AM 0 Test.cs
1/6/2003 7:55:14 AM 7 test.dll
11/14/2002 4:54:02 PM 8 transcmdlet.dll
7/12/2002 8:08:08 PM 28 TTest.exe
6/23/2003 11:01:10 AM 32 types.xml
6/2/2003 10:15:51 AM 1 uhl0ddmu.txt
7/12/2002 8:08:28 PM 14 UnitTestFramework.dll
7/12/2002 8:30:20 PM 40 unittestframework.pdb
1/13/2003 7:55:07 PM 76 URA.dll
8/8/2002 7:00:26 PM 20 vmrdx.xml
1/14/2003 5:55:07 PM 44 virtualdrive.dll
1/14/2003 5:55:07 PM 200 virtualdrive.pdb
12/10/2002 10:49:24 AM 260 win32cmdx.dll
1/9/2003 6:55:23 PM 1,230 win32cmds.pdb
12/10/2002 10:49:24 AM 92 winout.dll
2/8/2004 4:51:24 PM 64 winout.pdb
1/22/2003 1:32:50 PM 0 1033
1/24/2003 9:51:27 PM 0 test

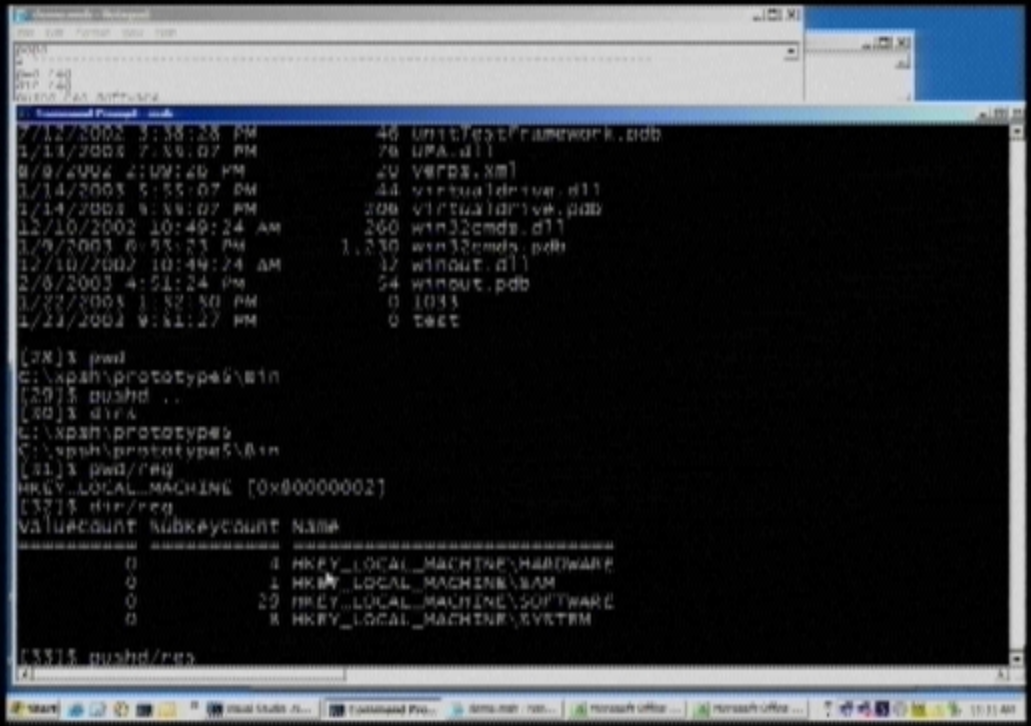


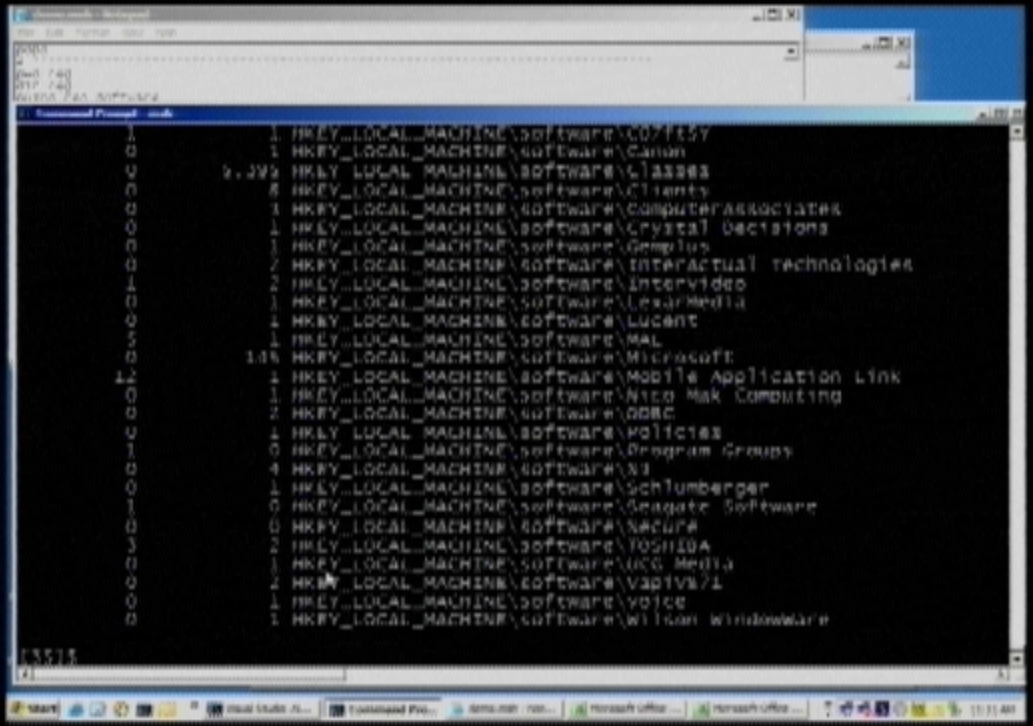

Command Prompt - cmd
</PROPERTY>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">winout.bob</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Written">
<VALUE TYPE="System.DateTime">1/22/2003 1:12:50 PM</VALUE>
</PROPERTY>
<PROPERTY NAME="Length.hb">
<VALUE TYPE="System.Int64">0</VALUE>
</PROPERTY>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">lll</VALUE>
</PROPERTY>
</INSTANCE>
<INSTANCE>
<PROPERTY NAME="Written">
<VALUE TYPE="System.DateTime">1/21/2003 9:41:27 PM</VALUE>
</PROPERTY>
<PROPERTY NAME="Length.hb">
<VALUE TYPE="System.Int64">0</VALUE>
</PROPERTY>
<PROPERTY NAME="Name">
<VALUE TYPE="System.String">test</VALUE>
</PROPERTY>
</INSTANCE>
</CIM>
[1/1]$

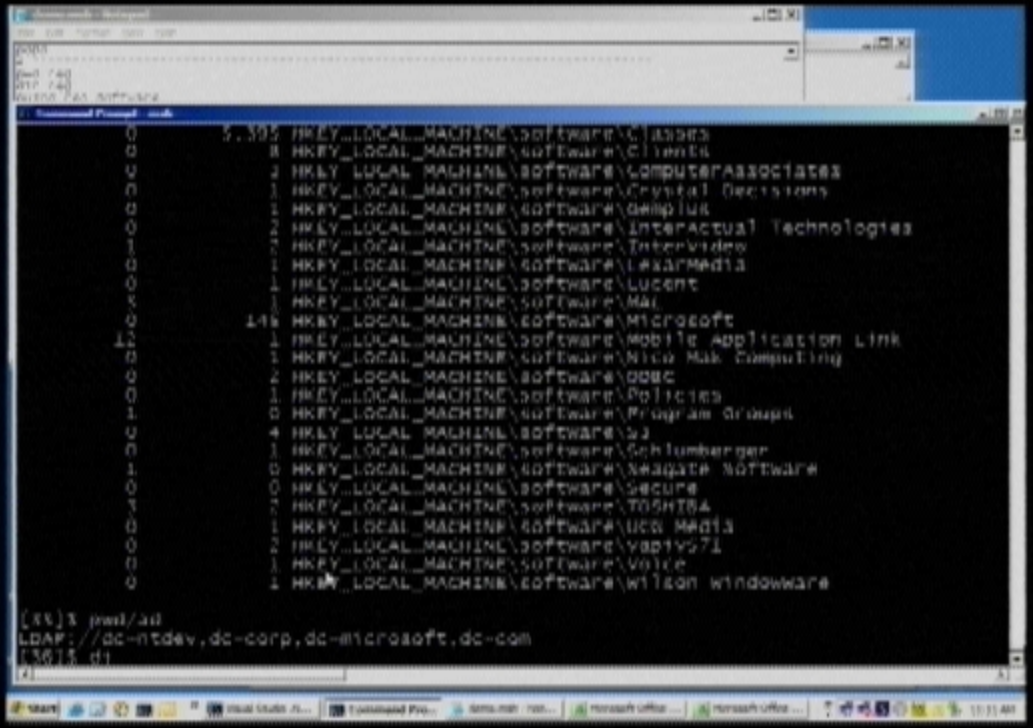

11/26/2002 10:13:56 AM 13 t1.htm
11/26/2002 10:13:44 AM 0 t1.html
4/24/2003 12:12:00 PM 0 t1.man
2/13/2003 12:13:40 PM 0 t1.txt
10/14/2002 4:11:22 PM 1 t1.xml
8/8/2002 2:09:30 PM 66 TaskScheduler.dll
3/4/2003 4:00:38 PM 0 test.bat
1/6/2004 10:21:21 AM 4 test.cs
5/6/2003 7:55:14 AM 7 test.dll
11/14/2002 4:54:07 PM 8 TransCmdLet.dll
7/12/2002 3:38:20 PM 28 treat.exe
6/25/2003 11:01:16 AM 35 types.xml
6/2/2004 10:16:31 AM 1 uhlddms.txt
7/12/2002 3:38:20 PM 13 unittestframework.dll
7/12/2002 3:38:28 PM 46 UnitTestFramework.pdb
1/14/2003 7:56:07 PM 78 UPA.dll
8/8/2002 2:08:26 PM 20 vars.xml
1/14/2003 6:55:07 PM 44 virtualdrive.dll
1/14/2003 6:56:07 PM 208 virtualdrive.pdb
12/10/2002 10:49:24 AM 260 win32cmds.dll
1/9/2003 6:55:23 PM 1,350 win32cmds.pdb
12/10/2002 10:49:24 AM 12 winout.dll
2/8/2003 4:51:24 PM 54 winout.pdb
1/27/2003 1:52:50 PM 0 1033
1/23/2003 9:51:27 PM 0 test
[JK]% pwd
c:\xpah\prototype6\bin
[JK]%

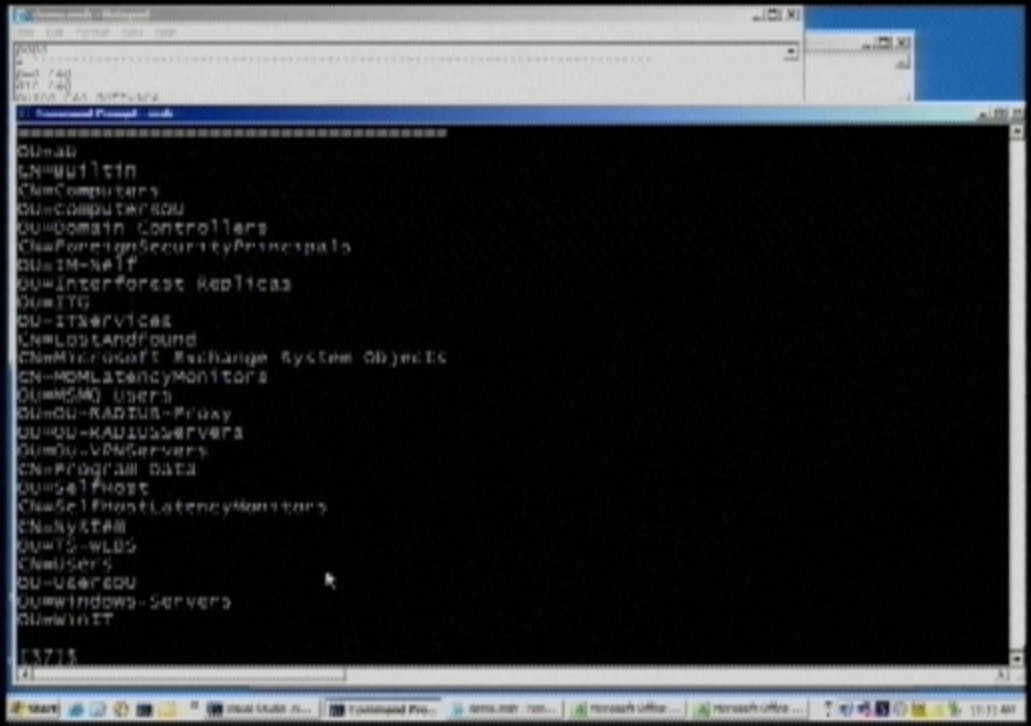

[20]$ pwd
c:\xpsh\prototype5\bin
[20]$ pushd ..
[30]$ dirs
c:\xpsh\prototype5
c:\xpsh\prototype5\bin
[31]$

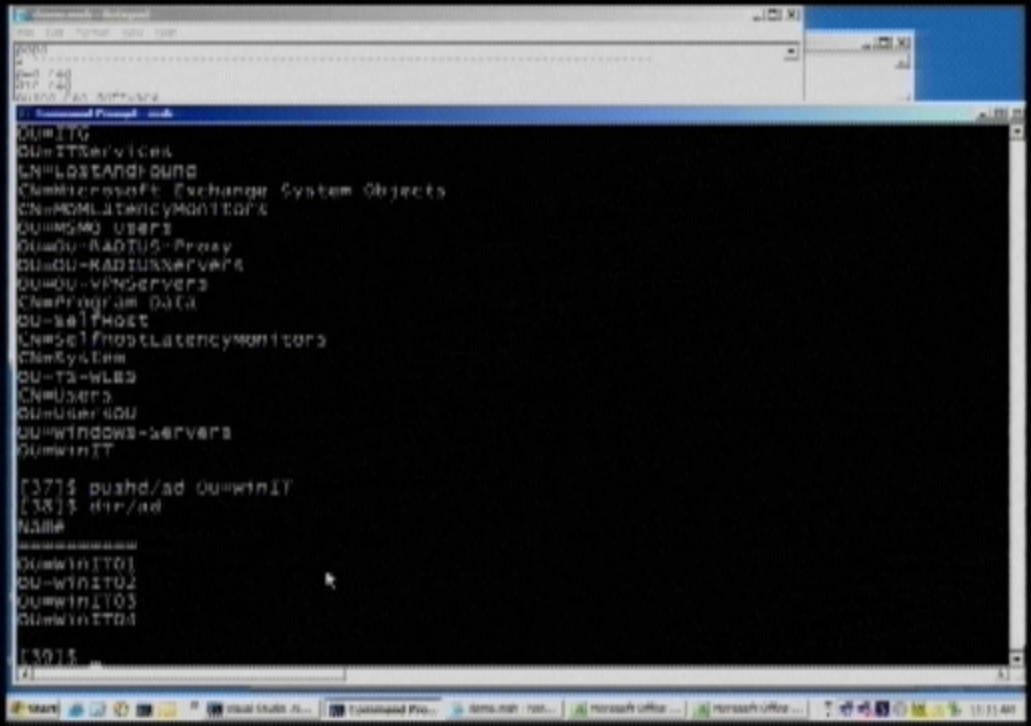

11/12/2002 5:38:28 PM 46 UnitTest\framework.pdb
1/11/2001 7:55:07 PM 76 UPA.dll
8/8/2002 2:00:40 PM 20 verds.xml
1/14/2001 5:55:07 PM 44 virtualdrive.dll
1/14/2001 5:55:07 PM 208 virtualdrive.pdb
12/10/2002 10:49:24 AM 260 win32cmds.dll
1/9/2001 6:55:21 PM 1,720 win32cmds.pdb
12/10/2002 10:49:24 AM 12 winout.dll
2/8/2003 4:51:24 PM 24 winout.pdb
1/27/2001 1:52:50 PM 0 1033
1/23/2002 9:51:27 PM 0 test
[3K]% pwd
C:\xpsh\prototype5\bin
[20]% pushd ..
[20]% dirA
C:\xpsh\prototype5
C:\xpsh\prototype5\bin
[21]% pwd/reg
HKEY_LOCAL_MACHINE [0x80000002]
[37]% dir/reg
ValueCount SubKeyCount NAME
0 4 HKEY_LOCAL_MACHINE\HARDWARE
0 1 HKEY_LOCAL_MACHINE\SAM
0 29 HKEY_LOCAL_MACHINE\SOFTWARE
0 8 HKEY_LOCAL_MACHINE\SYSTEM
[33]%


11/12/2002 5:38:28 PM 46 unittest\framework.pdb
1/14/2003 7:55:07 PM 78 UPA.dll
8/8/2002 2:08:46 PM 20 verb%.xml
1/14/2003 5:55:07 PM 44 virtualdrive.dll
1/14/2003 5:55:07 PM 208 virtualdrive.pdb
12/10/2002 10:49:24 AM 260 win32cmds.dll
1/9/2003 8:55:51 PM 1,220 win32cmds.pdb
12/10/2002 10:49:24 AM 12 winout.dll
2/8/2003 4:51:24 PM 54 winout.pdb
1/27/2003 1:52:50 PM 0 1033
1/23/2003 9:51:27 PM 0 test
[3K]% pwd
C:\xpsh\prototype5\bin
[29]% pushd ..
[30]% dir*
C:\xpsh\prototype5
C:\xpsh\prototype5\bin
[31]% pwd/reg
HKEY_LOCAL_MACHINE [0x80000002]
[32]% dir/reg
ValueCount SubKeyCount NAME
0 4 HKEY_LOCAL_MACHINE\HARDWARE
0 1 HKEY_LOCAL_MACHINE\SAM
0 29 HKEY_LOCAL_MACHINE\SOFTWARE
0 8 HKEY_LOCAL_MACHINE\SYSTEM
[33]% pushd/reg


HKEY_LOCAL_MACHINE\software\Canon
HKEY_LOCAL_MACHINE\software\Clients
HKEY_LOCAL_MACHINE\software\ComputerAssociates
HKEY_LOCAL_MACHINE\software\Crystal Decisions
HKEY_LOCAL_MACHINE\software\Gemplus
HKEY_LOCAL_MACHINE\software\Interactual Technologies
HKEY_LOCAL_MACHINE\software\Intervideo
HKEY_LOCAL_MACHINE\software\LexarMedia
HKEY_LOCAL_MACHINE\software\Lucent
HKEY_LOCAL_MACHINE\software\MAL
HKEY_LOCAL_MACHINE\software\Microsoft
HKEY_LOCAL_MACHINE\software\Mobile Application Link
HKEY_LOCAL_MACHINE\software\Nico Mak Computing
HKEY_LOCAL_MACHINE\software\ODBC
HKEY_LOCAL_MACHINE\software\Policies
HKEY_LOCAL_MACHINE\software\Program Groups
HKEY_LOCAL_MACHINE\software\RA
HKEY_LOCAL_MACHINE\software\Schlumberger
HKEY_LOCAL_MACHINE\software\Seagate Software
HKEY_LOCAL_MACHINE\software\SAFER
HKEY_LOCAL_MACHINE\software\TOSHIBA
HKEY_LOCAL_MACHINE\software\UCG Media
HKEY_LOCAL_MACHINE\software\Vaplvl
HKEY_LOCAL_MACHINE\software\Voice
HKEY_LOCAL_MACHINE\software\Wilson WindowWare


HKEY_LOCAL_MACHINE\software\Classes
HKEY_LOCAL_MACHINE\software\Clients
HKEY_LOCAL_MACHINE\software\computerassociates
HKEY_LOCAL_MACHINE\software\Crystal Decisions
HKEY_LOCAL_MACHINE\software\Gemplus
HKEY_LOCAL_MACHINE\software\Interactual Technologies
HKEY_LOCAL_MACHINE\software\InterVideo
HKEY_LOCAL_MACHINE\software\Lexarmedia
HKEY_LOCAL_MACHINE\software\Lucent
HKEY_LOCAL_MACHINE\software\MAI
HKEY_LOCAL_MACHINE\software\Microsoft
HKEY_LOCAL_MACHINE\software\Mobile Application Link
HKEY_LOCAL_MACHINE\software\Nico Mak Computing
HKEY_LOCAL_MACHINE\software\ODBC
HKEY_LOCAL_MACHINE\software\Policies
HKEY_LOCAL_MACHINE\software\Program Groups
HKEY_LOCAL_MACHINE\software\SJ
HKEY_LOCAL_MACHINE\software\Schlumberger
HKEY_LOCAL_MACHINE\software\Seagate Software
HKEY_LOCAL_MACHINE\software\Secure
HKEY_LOCAL_MACHINE\software\TOSHIBA
HKEY_LOCAL_MACHINE\software\UGS MAGIX
HKEY_LOCAL_MACHINE\software\vap1y571
HKEY_LOCAL_MACHINE\software\Voice
HKEY_LOCAL_MACHINE\software\Wilson Windowware
[%]% pwd/ad
LDAP://dc-ntdev,dc-corp,dc-microsoft,dc-com


Command Prompt
OU=AD
CN=Builtin
CN=Computers
OU=Computer OU
OU=Domain Controllers
CN=ForeignSecurityPrincipals
OU=IM-Self
OU=Interforest Replicas
OU=ITG
OU-ITServices
CN=LostAndFound
CN=Microsoft Exchange System Objects
CN=MOMLatencyMonitors
OU=MSMQ Users
OU=OU-RADIUS-Proxy
OU=OU-RAUIUSServers
OU=OU-VPNServers
CN=ProgramData
OU=SelfHost
CN=SelfHostLatencyMonitors
CN=SkyDrive
OU=TS-WLBS
CN=Users
OU-UserOU
OU=Windows-Servers
OU=WinIT


OU=ITG
OU=ITServices
CN=LostAndFound
CN=MicrosoftExchangeSystemObjects
CN=MDMLatencyMonitors
OU=MSMQ Users
OU=OU-RADIUSProxy
OU=OU-RADIUSServers
OU=OU-VPNServers
CN=ProgramData
OU=SelfHost
CN=SelfHostLatencyMonitors
CN=System
OU=TS-WLBS
CN=Users
OU=UserOU
OU=WindowsServers
OU=winIT
[37]$ pushd/ad OU=winIT
[%]$ dir/ad
NAME
OU=winIT01
OU=winIT02
OU=winIT03
OU=winIT04
[30]$